

SIMATIC

S7-1200 G2 Programmable Logic Controller

System Manual

Introduction

1

Industrial cybersecurity

2

Product overview

3

Installation and wiring

4

PLC concepts, configuration,
and programming

5

Protection

6

Communication

7

Near Field Communication
(NFC)

8

Web server

9

Motion control

10

PID

11

Online and diagnostic tools

12

Technical specifications

A

Ordering information

B

Safety-relevant symbols

C

Continued

Comparison to S7-1200

D

SIMATIC S7-1200 G2 data

E

S7-1200 G2 Programmable Logic Controller

System Manual

Legal information

Warning notice system

This manual contains notices you have to observe in order to ensure your personal safety, as well as to prevent damage to property. The notices referring to your personal safety are highlighted in the manual by a safety alert symbol, notices referring only to property damage have no safety alert symbol. These notices shown below are graded according to the degree of danger.

DANGER

indicates that death or severe personal injury **will** result if proper precautions are not taken.

WARNING

indicates that death or severe personal injury **may** result if proper precautions are not taken.

CAUTION

indicates that minor personal injury can result if proper precautions are not taken.

NOTICE

indicates that property damage can result if proper precautions are not taken.

If more than one degree of danger is present, the warning notice representing the highest degree of danger will be used. A notice warning of injury to persons with a safety alert symbol may also include a warning relating to property damage.

Qualified Personnel

The product/system described in this documentation may be operated only by **personnel qualified** for the specific task in accordance with the relevant documentation, in particular its warning notices and safety instructions. Qualified persons are those who, because of their training and experience, are familiar with the installation, assembly, commissioning, operation, decommissioning and disassembly of the product and can recognize risks and avoid possible hazards.

Proper use of Siemens products

Note the following:

WARNING

Siemens products may only be used for the application described in the catalog and the associated usage information. If products and components from other manufacturers are used, these must be recommended or approved by Siemens. Proper transport, storage, installation, assembly, commissioning, operation and maintenance are required to ensure that the products operate safely and without any problems. The permissible ambient conditions must be complied with. The information in the relevant documentation must be observed.

Trademarks

All names identified by ® are registered trademarks of Siemens Aktiengesellschaft. The remaining trademarks in this publication may be trademarks whose use by third parties for their own purposes could violate the rights of the owner.

Disclaimer of Liability

We have reviewed the contents of this publication to ensure consistency with the hardware and software described. Since variance cannot be precluded entirely, we cannot guarantee full consistency. However, the information in this publication is reviewed regularly and any necessary corrections are included in subsequent editions.

Table of contents

1	Introduction.....	14
1.1	General information.....	14
1.2	Maintaining operational safety of your plant.....	16
1.3	S7-1200 G2 documentation guide.....	17
1.4	SIMATIC Technical Documentation.....	18
1.5	Tool support.....	20
2	Industrial cybersecurity.....	22
2.1	Cybersecurity information.....	22
2.2	Security update notification.....	23
2.3	Basic information on industrial cybersecurity.....	23
2.3.1	Definition of industrial cybersecurity.....	23
2.3.2	Objectives of industrial cybersecurity.....	24
2.4	Integrated security concept and security strategies.....	24
2.4.1	Comprehensive security concept "Defense in Depth".....	24
2.4.2	Security management.....	25
2.5	Operational application environment and security assumptions.....	27
2.5.1	Intended use.....	27
2.5.2	Requirements for the operational application environment and security assumptions...	28
2.6	Security properties of the devices.....	29
2.7	Secure operation of the system.....	29
2.7.1	Hardening measures.....	29
2.7.2	Secure configuration.....	29
2.7.3	Access control.....	30
2.7.4	Handling of sensitive data.....	30
2.7.5	Regular firmware updates.....	31
2.7.6	Notifications about security vulnerabilities (Siemens Security Advisories).....	31
2.7.7	Data backup.....	32
2.7.8	Security checks.....	32
2.7.9	Secure decommissioning.....	32
2.7.9.1	Securely removing data.....	32
2.7.9.2	Recycling and disposal.....	35
2.8	Secure operation of the engineering software.....	36
2.9	Secure operation of the CPUs.....	36
2.9.1	Secure configuration.....	36
2.9.2	User management and access control.....	36
2.9.2.1	Administration of user accounts.....	36
2.9.2.2	Assigning secure passwords.....	36
2.9.2.3	Password management.....	37
2.9.2.4	Setting protection levels.....	38

2.9.2.5	Certificate management.....	38
2.9.3	Protection functions.....	38
2.9.4	Signed firmware update for CPUs.....	39
2.9.5	Secure Boot for CPUs.....	40
2.9.6	Secure communication/OPC UA.....	40
2.9.7	Sensitive data.....	40
2.9.8	Backups and data backups.....	41
2.9.9	Additional protective measures for network security.....	41
2.9.10	Using a Web server.....	42
2.9.11	Recording security events.....	42
2.9.12	Syslog messages.....	43
2.9.12.1	Transfer of the syslog messages to a syslog server.....	45
2.9.12.2	Structure of the Syslog messages.....	48
2.10	Secure operation of interface modules.....	50
2.10.1	Data integrity for interface modules.....	50
2.10.2	Signed firmware update for interface modules.....	52
2.10.3	Secure Boot for interface modules.....	53
2.11	Secure operation of I/O modules.....	54
2.11.1	Data integrity for I/O modules.....	54
2.11.2	Signed firmware update for I/O modules.....	55
2.12	Secure operation of power supply modules.....	56
2.12.1	Signed firmware update for system power supplies (PS).....	56
3	Product overview.....	57
3.1	Introducing the S7-1200 G2 PLC.....	57
3.2	S7-1200 G2 modules and boards.....	59
3.3	Features.....	61
3.4	What's new?.....	62
4	Installation and wiring.....	63
4.1	Installation guidelines.....	63
4.2	Safety information.....	65
4.3	Mounting dimensions.....	67
4.4	Providing power for the CPU.....	68
4.5	Expansion capability of the CPU.....	71
4.6	Installation and removal procedures.....	71
4.6.1	Installing and removing a CPU.....	71
4.6.2	Installing and removing expansion modules.....	74
4.6.3	Installing and removing expansion boards.....	77
4.6.4	Removing and installing terminal block connectors.....	79
4.7	Wiring guidelines and procedures.....	83
4.7.1	Safety considerations.....	83
4.7.2	Guidelines for isolation.....	84
4.7.3	Guidelines for grounding.....	86

4.7.4	Guidelines for wiring.....	87
4.7.5	Wiring and unwiring terminal block connectors.....	88
4.7.6	Guidelines for inductive loads.....	94
4.7.7	Guidelines for lamp loads.....	96
4.8	Maintenance and repair.....	96
5	PLC concepts, configuration, and programming.....	97
5.1	TIA Portal.....	97
5.2	Different views in the TIA Portal.....	97
5.3	Using the TIA Portal Information System.....	99
5.4	Program structure.....	99
5.4.1	Structure of a STEP 7 user program.....	99
5.4.2	Execution of the user program.....	101
5.4.3	Startup configuration and processing.....	103
5.4.4	Processing the scan cycle in RUN mode.....	105
5.4.5	Organization blocks (OBs).....	106
5.4.5.1	Program cycle OB.....	106
5.4.5.2	Startup OB.....	107
5.4.5.3	Time delay interrupt OB.....	107
5.4.5.4	Cyclic interrupt OB.....	107
5.4.5.5	Hardware interrupt OB.....	108
5.4.5.6	Time error interrupt OB.....	110
5.4.5.7	Diagnostic error interrupt OB.....	111
5.4.5.8	Pull or plug of modules OB.....	113
5.4.5.9	Rack or station failure OB.....	114
5.4.5.10	Time of day OB.....	115
5.4.5.11	Synchronous cycle OB.....	116
5.4.5.12	Status OB.....	116
5.4.5.13	Update OB.....	117
5.4.5.14	Profile OB.....	117
5.4.5.15	MC-Servo and MC-Interpolator OB.....	117
5.4.5.16	MC-PreInterpolator.....	118
5.4.5.17	MC-PreServo.....	119
5.4.5.18	MC-PostServo.....	119
5.4.5.19	MC-LookAhead.....	120
5.4.5.20	Programming error OB.....	121
5.4.5.21	I/O access error OB.....	122
5.4.5.22	Event execution priorities and queuing.....	123
5.4.6	Monitoring and configuring the cycle time.....	126
5.4.7	Cycle time and communication load.....	128
5.4.8	CPU memory.....	129
5.4.8.1	Memory management.....	129
5.4.8.2	Notes about retentive memory.....	130
5.4.8.3	System and clock memory.....	131
5.4.9	Diagnostics buffer.....	133
5.4.10	Program alarms.....	134
5.4.11	Time of day clock.....	135
5.4.12	Data storage, memory areas, I/O and addressing.....	136
5.4.12.1	Accessing the data of the CPU.....	136
5.4.12.2	Using absolute addressing to access CPU data.....	137

5.4.12.3	Addressing the local and expansion I/O.....	140
5.4.13	Processing of analog values.....	141
5.4.14	Using a memory card.....	142
5.4.14.1	Memory cards.....	142
5.4.14.2	Inserting a memory card in the CPU.....	144
5.4.14.3	Empty memory card.....	145
5.4.14.4	Configuring the startup parameter of the CPU before copying the project to the memory card	145
5.4.14.5	Transfer card.....	146
5.4.14.6	Program card.....	148
5.4.14.7	Firmware update card.....	152
5.4.14.8	Memory card for protecting confidential PLC configuration data.....	154
5.4.14.9	Recovery from a lost password.....	156
5.4.14.10	Memory card for copying license conditions and copyrights from the CPU.....	156
5.4.14.11	Using a memory card with the S7-1200 G2 fail-safe CPU.....	157
5.5	Managing users and roles.....	158
5.6	Device configuration.....	158
5.6.1	Overview.....	158
5.6.2	Inserting a CPU.....	159
5.6.3	Uploading the configuration of a connected CPU.....	162
5.6.4	Adding modules to the configuration.....	165
5.6.5	Configuring the operation of the CPU.....	166
5.6.5.1	Configuring the system power supply.....	169
5.6.5.2	Pulse catch.....	169
5.6.6	Configuring the parameters of the modules.....	171
5.6.7	Configuring the CPU for communication.....	173
5.6.8	Time synchronization.....	175
5.7	Compatibility between STEP 7 versions and the S7-1200 G2 CPU.....	177
5.8	Instruction set	178
5.8.1	Supported programming languages.....	178
5.8.2	Instructions for programming the PLC.....	178
5.8.3	Basic instructions.....	179
5.8.4	Extended instructions.....	180
5.8.5	Technology instructions.....	182
5.8.6	Communication instructions.....	183
5.8.7	Optional instructions.....	184
6	Protection.....	185
6.1	Overview of the protection functions.....	185
6.2	Protection of confidential configuration data.....	188
6.3	Local user management.....	188
6.3.1	Useful information on the local user administration and access control.....	188
6.3.2	Advantages of the local user administration and access control.....	191
6.3.3	Access levels and function rights.....	193
6.3.4	Important information when using the ENDIS_PW instruction.....	196
6.4	Central user management.....	197

6.4.1	Useful information on central user management and access control.....	197
6.4.2	Configuring central user management in the editor for users and roles.....	200
6.4.3	Configuring central user management for an S7-1200 G2 CPU.....	203
6.4.4	Logon of central users.....	204
6.5	Configuring access protection for the CPU.....	206
6.6	Know-how protection.....	210
6.7	Using the user program to set additional access protection.....	213
7	Communication.....	214
7.1	Overview.....	214
7.2	Secure communication.....	215
7.3	Communication protocols and ports used by Ethernet communication.....	216
7.4	Asynchronous communication connections.....	218
7.5	Supported certificates.....	220
7.6	PROFINET.....	220
7.6.1	CPU communication.....	220
7.6.2	Creating a network connection.....	222
7.6.3	Configuring the Local/Partner connection path.....	223
7.6.4	Locating the Ethernet (MAC) address on the CPU.....	223
7.6.5	Assigning Internet Protocol (IP) addresses.....	224
7.6.5.1	Assigning IP addresses to programming and network devices.....	224
7.6.5.2	Checking the IP address and MAC address of your network interface.....	225
7.6.5.3	Assigning an IP address to an online CPU.....	226
7.6.5.4	Configuring an IP address for a CPU in your project.....	227
7.6.6	Testing the PROFINET network.....	233
7.6.7	PROFINET device startup time, naming, and address assignment.....	234
7.6.8	Configuring Network Time Protocol (NTP) synchronization.....	235
7.6.9	Open user communication.....	235
7.6.9.1	Protocols.....	235
7.6.9.2	TCP, ISO on TCP, and UDP.....	236
7.6.9.2.1	TCP.....	236
7.6.9.2.2	ISO on TCP.....	236
7.6.9.2.3	UDP.....	237
7.6.9.3	Ad hoc mode.....	237
7.6.9.4	Instructions.....	238
7.6.9.5	Connection IDs for the Open user communication instructions.....	239
7.6.9.6	Parameters for the OUC connection.....	239
7.6.9.7	Transport Layer Security (TLS).....	240
7.6.9.8	Configuring DNS.....	240
7.6.9.9	Configuring an OUC connection in the TIA Portal.....	241
7.6.9.10	Common parameters for instructions.....	241
7.6.9.11	Restricted TSAPs or port numbers for passive ISO and TCP communication.....	242
7.6.10	Communication with a programming device.....	242
7.6.10.1	Establishing the hardware communications connection.....	243
7.6.10.2	Configuring the devices.....	244
7.6.10.3	Testing the PROFINET network.....	245
7.6.10.4	Assigning Internet Protocol (IP) addresses.....	246
7.6.11	PLC-to-PLC communication.....	248

7.6.11.1	Configuring connection parameters.....	249
7.6.11.2	Configuring transmit (send) and receive parameters.....	249
7.6.12	Configuring a CPU and PROFINET IO device.....	250
7.6.12.1	Adding a PROFINET IO device.....	250
7.6.12.2	Assigning CPUs and device name.....	251
7.6.12.3	Assigning Internet Protocol (IP) addresses.....	251
7.6.12.4	Configuring the IO cycle time.....	252
7.6.12.5	Prioritized startup of an IO device.....	252
7.6.13	Configuring a CPU and PROFINET I-device.....	253
7.6.13.1	I-device functionality.....	253
7.6.13.2	Properties and advantages of the I-device.....	254
7.6.13.3	Characteristics of an I-device.....	255
7.6.13.4	Data exchange between higher- and lower-level IO system.....	258
7.6.13.5	Configuring the I-device.....	260
7.6.14	Shared device functionality.....	263
7.6.15	Media Redundancy Protocol (MRP).....	264
7.6.16	Media Redundancy with Planned Duplication of frames (MRPD).....	264
7.6.17	S7 routing.....	265
7.6.18	Isochronous Real-Time PROFINET (IRT).....	265
7.6.19	SNMP.....	265
7.7	S7 communication.....	267
7.7.1	PUT and GET (Write and read from a remote CPU).....	267
7.7.2	Creating an S7 connection.....	269
7.7.3	PUT/GET connection parameter assignment.....	269
7.7.3.1	Connection ID parameter.....	270
7.7.3.2	Connection name parameter.....	271
7.8	Diagnostic events for distributed I/O.....	271
7.9	What to do when you cannot access the CPU by the IP address.....	272
7.10	OPC UA server.....	273
7.10.1	OPC UA Server method instructions.....	273
7.10.2	Limitations of the OPC UA server.....	274
7.10.3	OPC UA server security.....	275
7.11	Communication Processor (CP).....	276
7.11.1	CP 1243-1.....	276
7.11.2	Further information.....	276
7.12	Point-to-point (PtP) communication.....	277
7.12.1	Overview.....	277
7.12.2	Using the serial communication interfaces.....	277
7.12.3	Biasing and terminating an RS422 or RS485 network connector.....	278
7.12.4	PtP, Freeport communication.....	281
7.12.5	Configuring the PtP Freeport communication.....	282
7.12.5.1	Configuring the communication ports.....	282
7.12.5.2	Managing flow control.....	285
7.12.5.3	Configuring transmit (send) and receive parameters.....	287
7.12.5.4	Configuring transmit (send) parameters.....	287
7.12.5.5	Configuring receive parameters.....	289
7.12.6	3964(R) communication.....	295
7.12.7	Configuring the 3964(R) communication.....	297
7.12.7.1	Configuring the 3964(R) communication ports.....	297

7.12.7.2	Configuring the 3964(R) priority and protocol parameters.....	299
7.12.8	Point-to-Point Instructions.....	300
7.12.9	Programming the PtP communications.....	301
7.12.9.1	Programming overview.....	301
7.12.9.2	Polling architecture.....	302
7.13	Universal serial interface (USS) communication.....	303
7.13.1	USS instructions.....	305
7.13.2	USS status codes.....	306
7.13.3	USS general drive setup requirements.....	307
7.14	Modbus communication.....	308
7.14.1	Modbus TCP.....	309
7.14.1.1	Modbus TCP Instructions.....	310
7.14.1.1.1	Modbus TCP Redundancy instructions.....	311
7.14.2	Modbus RTU.....	312
7.14.2.1	Modbus RTU instructions and versions.....	313
7.14.2.2	Maximum number of supported Modbus slaves.....	314
8	Near Field Communication (NFC).....	315
9	Web server.....	316
9.1	Certificate requirements for the Web server.....	317
10	Motion control.....	318
10.1	Introducing S7-1200 G2 Motion Control.....	318
10.2	Motion Control Technology Objects (TOs).....	319
10.3	Motion Control instructions.....	321
10.4	Motion Control Organization Blocks (OBs).....	323
10.5	Differences between S7-1200 G2 and S7-1500/S7-1500T.....	324
10.5.1	Adapting Motion Control to S7-1200 G2.....	325
10.6	Additional information.....	326
11	PID.....	327
11.1	PID functionality.....	327
12	Online and diagnostic tools.....	329
12.1	Status LEDs.....	331
12.2	CPU error behavior.....	336
12.3	Analog module diagnostics.....	337
12.4	Comparing offline and online CPUs.....	338
12.5	Monitoring and modifying values in the CPU.....	338
12.5.1	Overview of the online monitoring and modification tools.....	338
12.5.2	Watch tables for monitoring the user program.....	339
12.5.3	Using the force table.....	339

12.6	Downloading in RUN mode.....	340
12.6.1	Overview.....	340
12.6.2	Prerequisites for "Download in RUN mode".....	341
12.6.3	Changing your program in RUN mode.....	341
12.6.4	Downloading selected blocks.....	342
12.6.5	Downloading a single selected block with a compile error in another block.....	344
12.6.6	Modifying and downloading existing tags in RUN mode.....	345
12.6.7	System reaction if the download process fails.....	348
12.6.8	Considerations when downloading in RUN mode	348
12.7	Tracing and recording CPU data on trigger conditions.....	350
12.8	Determining the type of error from an analog module.....	352
12.9	Backup and restore options.....	354
A	Technical specifications.....	356
A.1	General technical specifications.....	356
A.2	Protection methods.....	368
A.3	CPU 1212C.....	369
A.3.1	General specifications and features.....	369
A.3.2	Performance.....	371
A.3.3	Blocks, timers, and counters.....	371
A.3.4	Communications.....	372
A.3.5	Power supply and sensor power.....	375
A.3.6	Digital inputs and outputs.....	376
A.4	CPU 1212FC.....	380
A.4.1	General specifications and features.....	380
A.4.2	Performance.....	383
A.4.3	Blocks, timers, and counters.....	383
A.4.4	Communications.....	384
A.4.5	Power supply and sensor power.....	387
A.4.6	Digital inputs and outputs.....	388
A.5	CPU 1214C.....	391
A.5.1	General specifications and features.....	391
A.5.2	Performance.....	393
A.5.3	Blocks, timers, and counters.....	394
A.5.4	Communications.....	395
A.5.5	Power supply and sensor power.....	398
A.5.6	Digital inputs and outputs.....	399
A.6	CPU 1214FC.....	403
A.6.1	General specifications and features.....	403
A.6.2	Performance.....	406
A.6.3	Blocks, timers, and counters.....	406
A.6.4	Communications.....	407
A.6.5	Power supply and sensor power.....	410
A.6.6	Digital inputs and outputs.....	411
A.7	Digital signal modules (SMs).....	414
A.7.1	SM 1221 DI 16x24VDC.....	414
A.7.2	SM 1222 DQ 16x24VDC.....	416

A.7.3	SM 1222 DQ 16xRLY.....	418
A.7.4	SM 1223 DI 8x24VDC / DQ 8x24VDC.....	420
A.7.5	SM 1223 DI 8x24VDC / DQ 8xRLY.....	423
A.7.6	SM 1223 DI 16x24VDC / DQ 16x24VDC.....	425
A.7.7	SM 1223 DI 16x24VDC / DQ 16x24VDC Sink	428
A.7.8	SM 1223 DI 16x24VDC / DQ 16xRLY	430
A.8	Analog signal modules (SMs).....	433
A.8.1	SM 1231 AI 8x14bit.....	433
A.8.2	SM 1232 AQ 8x14bit.....	436
A.8.3	SM 1233 AI 4x14bit / AQ 4x14bit.....	438
A.8.4	Step response of the analog inputs.....	442
A.8.5	Sample time and update times for the analog inputs.....	442
A.8.6	Measurement ranges of the analog inputs for voltage and current.....	442
A.8.7	Measurement ranges of the analog outputs for voltage and current.....	443
A.8.8	Basic operation of a thermocouple.....	444
A.8.9	SM 1231 AI 8xTC	445
A.8.10	SM 1231 AI 4xRTD.....	450
A.9	Digital signal boards (SBs).....	456
A.9.1	SB 1221 DI 8x24VDC.....	456
A.9.2	SB 1222 DQ 8x24VDC.....	458
A.9.3	SB 1223 DI 4x24VDC / DQ 4x24VDC.....	460
A.9.4	SB 1223 DI 4x5VDC / DQ 4x5VDC.....	463
A.10	Analog signal boards (SBs).....	466
A.10.1	SB 1231 AI 4x14bit.....	466
A.10.2	SB 1232 AQ 4x14bit.....	468
A.10.3	SB 1233 AI 2x14bit / AQ 2x14bit.....	470
A.10.4	Step response of the analog inputs.....	474
A.10.5	Sample time and update times for the analog inputs.....	475
A.10.6	Measurement ranges of the analog inputs for voltage and current.....	475
A.10.7	Measurement ranges of the analog outputs for voltage and current.....	476
A.10.8	Basic operation of a thermocouple.....	477
A.10.9	SB 1231 AI 4xTC	478
A.10.10	SB 1231 AI 2xRTD.....	482
A.11	Battery board (BB) 1297.....	488
A.12	Communication interfaces.....	489
A.12.1	CP 1243-1.....	489
A.12.2	CM 1241 RS232/422/485.....	491
A.12.3	CB 1241 RS485	493
A.13	Input simulators.....	495
A.14	Companion products.....	497
A.14.1	Power module (PM) 1207.....	497

B	Ordering information.....	498
B.1	CPUs.....	498
B.2	Signal modules (SMs).....	498
B.3	Signal boards (SBs).....	499
B.4	Battery board (BB).....	499
B.5	Communication.....	499
B.6	Memory cards.....	500
B.7	Spare parts and other hardware.....	500
B.8	Terminal block spare kits.....	501
B.9	Programming software.....	503
C	Safety-relevant symbols.....	504
C.1	Devices without explosion protection.....	504
C.2	Devices with explosion protection.....	505
D	Comparison to S7-1200.....	507
E	SIMATIC S7-1200 G2 data.....	513
E.1	CPU data.....	513
E.2	Data of the interface and I/O modules.....	515
	Glossary.....	518
	Index.....	521

Introduction

1.1 General information

Purpose of the documentation

The S7-1200 G2 programmable logic controllers (PLCs) can control a variety of automation applications. Compact design, affordable price, and a powerful instruction set make the S7-1200 G2 CPU and modules a perfect solution for controlling a wide variety of applications. Together with the STEP 7 configuration and programming tool [\(Page 97\)](#), you have the flexibility you need to design your automation solutions.

This documentation provides information about the S7-1200 G2 CPU and modules. It contains information for engineers, programmers, installers, and electricians.

Required basic knowledge

To understand this documentation, you need a general knowledge of automation and programmable logic controllers.

Validity of the documentation

This documentation applies to the S7-1200 G2 CPU family and G2 modules.

Refer to the technical specifications [\(Page 356\)](#) for each CPU and module in the S7-1200 G2 family.

Conventions

STEP 7: In this documentation, "STEP 7" is used as a synonym for all versions of the configuration and programming software "STEP 7 (TIA Portal)".

Also observe notes marked as follows:

NOTE

A note contains important information on the product described in the documentation, on the handling of the product, or on the section of the documentation to which particular attention should be paid.

ID link for the digital nameplate



The ID link is a globally unique identifier according to IEC 61406-1, which you will find as a QR code on your product.

The figure shows an example of an ID link for the CPU 1212C AC/DC/RLY.

You can recognize the ID link by the frame with a black frame corner at the bottom right. The ID link takes you to the digital nameplate of your product.

Scan the QR code on the product or on the packaging label with a smartphone camera, barcode scanner, or reader app. Access the ID link.

In the digital nameplate, you can find product data, manuals, declarations of conformity, certificates and other helpful information about your product.

Industry Mall

The Industry Mall is the catalog and order system of Siemens AG for automation and drive solutions on the basis of Totally Integrated Automation (TIA) and Totally Integrated Power (TIP).

You can find catalogs for all automation and drive products on the Internet (<https://mall.industry.siemens.com>).

Certifications and approvals

Refer to the technical specifications ([Page 356](#)) for details on certifications and approvals.

Glossary

The definitions in the glossary provide an easy first reference for understanding the terms in this documentation.

1.2 Maintaining operational safety of your plant

NOTE

Operators of plants with safety-related features must meet operational safety requirements. Suppliers must also take measures when monitoring products.

To stay up-to-date on the latest operational safety requirements, visit the Siemens Industry Online Support (<https://sieportal.siemens.com/en-ww/support>) site and subscribe to email notifications:

1. Follow one of the links below:
 - SIMATIC S7-1200 G2/SIMATIC S7-1200 G2 F (<https://support.industry.siemens.com/cs/us/en/ps/30068>)
 - Distributed I/O (<https://support.industry.siemens.com/cs/ww/en/ps/14029>)
 - STEP 7 TIA Portal (<https://support.industry.siemens.com/cs/ww/en/ps/14667>)
 2. To subscribe to notifications, select "email on update".
-

NOTE

To reduce the risks associated with malicious or counterfeit CPUs and modules, use only official sales channels, such as the following:

- Siemens Industry Mall
 - Official Siemens distributors
 - Country-specific official Siemens sales and distribution channels
-

NOTE

To reduce the risks associated with compromised CPU or module firmware, only download firmware from the Siemens Industry Online Support website and verify the file integrity against the associated published SHA checksum.

NOTE

To reduce the risk of physical tampering with critical industrial equipment, implement the measures defined in the Operational guidelines (<https://www.siemens.com/global/en/products/services/cert/news/operational-guidelines-for-industrial-security.html>).

NOTE

For additional security, the CPU uses firmware encryption. While encryption provides confidentiality of the firmware, the main purpose is to enhance the secure boot process.

1.3 S7-1200 G2 documentation guide

S7-1200 G2 and the TIA Portal provide a variety of documentation and other resources for finding the technical information that you require.

- The S7-1200 G2 Programmable Logic Controller System Manual provides specific information about the operation, programming, and the specifications for the complete S7-1200 G2 product family.

The system manual is available on Siemens Industry Online Support (<https://support.industry.siemens.com/>) in multiple display formats and languages.

- The TIA Portal Information System provides access to the conceptual information and specific instructions that describe the operation and functionality of the programming package and basic operation of SIMATIC CPUs.
- You can also follow or join product discussions on the Service & Support technical forum (<https://support.industry.siemens.com/tf/ww/en/?Language=en&siteid=csius&treeLang=en&groupid=4000002&extranet=standard&viewreg=WW&nodeid0=34612486>). These forums allow you to interact with various product experts.
 - Forum for S7-1200 G2 (<https://support.industry.siemens.com/tf/ww/en/threads/237?title=simatic-s7-1200&skip=0&take=10&orderBy=LastPostDate+desc>)
 - Forum for TIA Portal (<https://support.industry.siemens.com/tf/ww/en/threads/243?title=step-7-tia-portal&skip=0&take=10&orderBy=LastPostDate+desc>)
- The SIMATIC Industrial Software SIMATIC Safety - Configuring and Programming Manual (<http://support.automation.siemens.com/WW/view/en/54110126/0/en>) provides information about configuring and programming fail-safe PLCs.

Contact your Siemens distributor or sales office for assistance in answering any technical questions, for training, or for ordering S7 products. Because sales representatives are technically trained and have knowledge about your operations, process and industry, as well as about the Siemens products that you are using, they can provide efficient answers to problems you might encounter.

System manual updates

When needed, changes and supplements to released system manuals are available in a system manual update document. These updates take precedence over the system manual. You can find the latest system manual updates on Siemens Industry Online Support (<https://support.industry.siemens.com/>)

1.4 SIMATIC Technical Documentation

Additional SIMATIC documents will complete your information. You can find these documents and their use at the following links and QR codes.

The Industry Online Support gives you the option to get information on all topics. Application examples support you in solving your automation tasks.

Overview of the SIMATIC Technical Documentation

Here you will find an overview of the SIMATIC documentation available in Siemens Industry Online Support:



Industry Online Support International

(<https://support.industry.siemens.com/cs/ww/en/view/109742705>)

Watch this short video to find out where you can find the overview directly in Siemens Industry Online Support and how to use Siemens Industry Online Support on your mobile device:



Quick introduction to the technical documentation of automation products per video (<https://support.industry.siemens.com/cs/us/en/view/109780491>)



YouTube video: Siemens Automation Products - Technical Documentation at a Glance (<https://youtu.be/TwLSxxRQsA>)

Retention of the documentation

Retain the documentation for later use.

For documentation provided in digital form:

1. Download the associated documentation after receiving your product and before initial installation/commissioning. Use the following download options:
 - Industry Online Support International: (<https://support.industry.siemens.com>)
The article number is used to assign the documentation to the product. The article number is specified on the product and on the packaging label. Products with new, non-compatible functions are provided with a new article number and documentation.
 - ID link:
Your product may have an ID link. The ID link is a QR code with a frame and a black frame corner at the bottom right. The ID link takes you to the digital nameplate of your product. Scan the QR code on the product or on the packaging label with a smartphone camera, barcode scanner, or reader app. Call up the ID link.
2. Retain this version of the documentation.

Updating the documentation

The documentation of the product is updated in digital form. In particular in the case of function extensions, the new performance features are provided in an updated version.

1. Download the current version as described above via the Industry Online Support or the ID link.
2. Also retain this version of the documentation.

mySupport

With "mySupport" you can get the most out of your Industry Online Support.

Registration	You must register once to use the full functionality of "mySupport". After registration, you can create filters, favorites and tabs in your personal workspace.
Support requests	Your data is already filled out in support requests, and you can get an overview of your current requests at any time.
Documentation	In the Documentation area you can build your personal library.
Favorites	You can use the "Add to mySupport favorites" to flag especially interesting or frequently needed content. Under "Favorites", you will find a list of your flagged entries.
Recently viewed articles	The most recently viewed pages in mySupport are available under "Recently viewed articles".
CAX data	The CAX data area gives you access to the latest product data for your CAX or CAE system. You configure your own download package with a few clicks: • Product images, 2D dimension drawings, 3D models, internal circuit diagrams, EPLAN macro files • Manuals, characteristics, operating manuals, certificates • Product master data

You can find "mySupport" on the Internet. (<https://support.industry.siemens.com/My/ww/en>)

Application examples

The application examples support you with various tools and examples for solving your automation tasks. Solutions are shown in interplay with multiple components in the system - separated from the focus on individual products.

You can find the application examples on the Internet.
(<https://support.industry.siemens.com/cs/ww/en/ps/ae>)

1.5 Tool support

Tools

The tools described below support you in all steps: from planning, over commissioning, all the way to analysis of your system.

TIA Selection Tool

The TIA Selection Tool tool supports you in the selection, configuration, and ordering of devices for Totally Integrated Automation (TIA).

As successor of the SIMATIC Selection Tools , the TIA Selection Tool assembles the already known configurators for automation technology into a single tool.

With the TIA Selection Tool , you can generate a complete order list from your product selection or product configuration.

You can find the TIA Selection Tool on the Internet.

(<https://support.industry.siemens.com/cs/us/en/view/109767888>)

SIMATIC Automation Tool

You can use the SIMATIC Automation Tool to perform commissioning and maintenance activities on various SIMATIC S7 stations as bulk operations independent of TIA Portal.

The SIMATIC Automation Tool offers a wide range of functions:

- Scanning of a PROFINET/Ethernet system network and identification of all connected CPUs
- Assignment of addresses (IP, subnet, Gateway) and device name (PROFINET device) to a CPU
- Transfer of the date and the programming device/PC time converted to UTC time to the module
- Program download to CPU
- RUN/STOP mode switchover
- CPU localization through LED flashing
- Reading out of CPU error information
- Reading the CPU diagnostic buffer
- Reset to factory settings
- Firmware update of the CPU and connected modules

You can find the SIMATIC Automation Tool on the Internet.

(<https://support.industry.siemens.com/cs/us/en/view/109986787>)

PRONETA

SIEMENS PRONETA (PROFINET network analysis) is a commissioning and diagnostic tool for PROFINET networks. PRONETA Basic has two core functions:

- In the network analysis, you get an overview of the PROFINET topology. Compare a real configuration with a reference installation or make simple parameter changes, e.g. to the names and IP addresses of the devices.
- The "IO test" is a simple and rapid test of the wiring and the module configuration of a plant, including documentation of the test results.

You can find SIEMENS PRONETA Basic on the Internet:

(<https://support.industry.siemens.com/cs/ww/en/view/67460624>)

SIEMENS PRONETA Professional is a licensed product that offers you additional functions. It offers you simple asset management in PROFINET networks and supports operators of automation systems in automatic data collection/acquisition of the components used through various functions:

- The user interface (API) offers an access point to the automation cell to automate the scan functions using MQTT or a command line.
- With PROFlenergy diagnostics, you can quickly detect the current pause mode or the readiness for operation of devices that support PROFlenergy and change these as needed.
- The data record wizard supports PROFINET developers in reading and writing acyclic PROFINET data records quickly and easily without PLC and engineering.

You can find SIEMENS PRONETA Professional on the Internet.

(<https://www.siemens.com/proneta-professional>)

SINETPLAN

SINETPLAN, the Siemens Network Planner, supports you in planning automation systems and networks based on PROFINET. The tool facilitates professional and predictive dimensioning of your PROFINET installation as early as in the planning stage. In addition, SINETPLAN supports you during network optimization and helps you to exploit network resources optimally and to plan reserves. This helps to prevent problems in commissioning or failures during productive operation even in advance of a planned operation. This increases the availability of the production plant and helps improve operational safety.

The advantages at a glance

- Network optimization thanks to port-specific calculation of the network load
- Increased production availability thanks to online scan and verification of existing systems
- Transparency before commissioning through importing and simulation of existing STEP 7 projects
- Efficiency through securing existing investments in the long term and the optimal use of resources

You can find SINETPLAN on the Internet

(<https://www.siemens.com/global/en/products/automation/industrial-communication/profinet/sinetplan.html>).

Industrial cybersecurity

Due to the digitalization and increasing networking of machines and industrial plants, the risk of cyber attacks is also growing. Appropriate protective measures are therefore mandatory, particularly in the case of critical infrastructure facilities.

In the first part of this section you will find basic information on the subject of industrial cybersecurity. Subsequent sections describe recommended measures for protecting the entire system and the individual components from manipulation and unwanted access.

NOTE

Security-relevant changes to software or devices are documented in the section New properties/functions ([Page 29](#)).

2.1 Cybersecurity information

Siemens provides products and solutions with industrial cybersecurity functions that support the secure operation of plants, systems, machines and networks.

In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial cybersecurity concept. Siemens' products and solutions constitute one element of such a concept.

Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place.

For additional information on industrial cybersecurity measures that may be implemented, please visit <https://www.siemens.com/cybersecurity-industry>.

Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are no longer supported, and failure to apply the latest updates may increase customer's exposure to cyber threats.

To stay informed about product updates, subscribe to the Siemens Industrial Cybersecurity RSS Feed under <https://new.siemens.com/cert>.

2.2 Security update notification

Read the special information on maintaining the operational safety of your plant in the Introduction (Page 16) section.

Set up notification of security updates

To receive notifications about security updates, proceed as follows:

1. Register with mySiePortal (<https://sieportal.siemens.com/en-ww/mysieportal>).
2. Enter the keyword "Security" in the search engine.
3. Choose the "Search in Knowledge base" option.
4. Enter the name or article number of the product in the product search.
5. Select the "Other types" option from the filter menu for "Type," and choose "Download" and "Product note".
6. For the document you want to be informed about, select "Add to my favorites" using the 3 dots on the right.

For example, if you would like to be informed about all firmware versions of the CPUs, select the entry "Firmware update S7-1500 CPUs incl. displays and ET 200 CPUs (ET 200SP, ET 200pro)".

7. In the following dialog, enter the name of the favorite, select the storage location, and select the "Notify me" option. Then click the "+ Add to my favorites" button.

Result: You will be notified by email each time the document is changed.

Under "mySiePortal" > "Lists & notifications" > "My notifications", you can display your notifications and delete them if necessary.

2.3 Basic information on industrial cybersecurity

2.3.1 Definition of industrial cybersecurity

Industrial cybersecurity is generally understood to mean all measures to protect against the following threats:

- Loss of confidentiality due to unauthorized access to data
- Loss of integrity due to manipulation of data
- Loss of availability (for example, due to the destruction of data or denial of service (DoS))

2.3.2 Objectives of industrial cybersecurity

The objectives of industrial cybersecurity are:

- Ensuring trouble-free operation of industrial plants and production processes
- Preventing threats to people and production from cybersecurity attacks
- Protection of industrial plants against espionage and manipulation
- Protection of industrial automation systems and components against unauthorized access and data loss
- Provision of a practical and cost-effective concept for securing existing plants and devices that do not have their own security functions
- Use of existing, open, and proven industrial cybersecurity standards
- Compliance with legal requirements

An optimized and adapted security concept applies to automation and drive technology. The security measures must not impede or endanger production.

2.4 Integrated security concept and security strategies

2.4.1 Comprehensive security concept "Defense in Depth"

With Defense in Depth, Siemens provides a multi-layer security concept that offers industrial plants comprehensive and far-reaching protection in accordance with the recommendations of the IEC 62443 international standard.

Productivity and know-how are protected on 3 levels:

Plant security

Plant security uses various methods to safeguard critical components from physical access by people. This starts with classic building access and extends to securing sensitive areas using access control (for example, code card, iris scan, fingerprint or access code).

Network security

Automation networks must be protected against unauthorized access. This is achieved through security measures on the product, but also those in the product-related environment.

System integrity

Targeted measures must be taken to protect existing know-how or to prevent unauthorized access to automation processes. The measures protect against unauthorized configuration changes, and highlight attempts at manipulation.

You can find more information on the topics of Defense in Depth, plant security, network security, and system integrity on the SIEMENS Industrial cybersecurity

(<https://www.siemens.com/us/en/company/topic-areas/cybersecurity/industrial-security.html>) Web page.

You can also visit the download center (https://cert-portal.siemens.com/operational-guidelines-industrial-security.pdf?ste_sid=0d5cc2df23db50211d4d0a3c7653cba7) to obtain more information on the topic of industrial cybersecurity. The "Operational Guidelines", for example, provide recommendations on basic security measures for secure machine and plant operation in an industrial environment.

2.4.2 Security management

The ISO 27001 and IEC 62443 standards call for a comprehensive approach in information technology (IT) and operational technology (OT) to protect against cyber attacks.

Responsibility for cybersecurity and IT security

Every operator of machinery and equipment is responsible for:

- Defining cybersecurity and IT security as an important criterion in the procurement and selection of machines and software applications
- Use of suitable measures to protect production resources, data, and communication from manipulation and theft
- Providing all necessary resources and training to employees to fully support these goals

For this purpose, suitable measures must be selected after a risk assessment and a cost-benefit analysis in order to protect material and intellectual property and prevent damage from occurring. These measures should be integrated into corporate processes and procedures, evaluated regularly, and firmly anchored in the corporate culture. In addition to protecting intellectual property, the protection of personal data must be ensured at all organizational units and levels.

Siemens will provide you with information and support. Subscribe to the Security feeds (<https://www.siemens.com/cert>) for information on vulnerabilities. Register with mySiePortal (<https://sieportal.siemens.com/en-ww/mysieportal>) and create filters to be notified when important information is published. The procedure is described in the section Notification of security updates (Page 23). Consider using Siemens Cybersecurity Services.

Responsibility in the digital supply chain

Cybersecurity should play a critical role in the evaluation and procurement process. The entire life cycle of a product should be considered to ensure protection against current and future risks. These include, for example, security updates throughout the product life cycle, including guidelines for secure disposal of the product.

Siemens plans and announces the provision of security updates, as well as total discontinuation of products, as part of product support.

Employee awareness

Regular training in cybersecurity and continuous testing of training success are essential so that cybersecurity measures are internalized in processes and work instructions. This involves general training in the use of software and IT hardware for company communication and as work equipment, for example:

- Secure handling of USB devices
- Encrypted communication
- Use of VPN
- Rules for passwords and use of access
- Setting up two-factor authentication
- Educating employees about the dangers posed by malware, phishing, social engineering and other factors

Furthermore, if applicable, production equipment and software training should always include the topic of cybersecurity.

Maintaining the security concept through updates

Keeping software up-to-date is essential, for example, to benefit from the following measures:

- Implementation of new security strategies, protocols and techniques
- Closing of security vulnerabilities
- Elimination of security vulnerabilities

To this end, it is necessary to keep a constant eye on the further development of protective measures and, if necessary, the expansion of requirements.

Recommendations:

- Set up notifications for (security) updates
- Subscribe to information on vulnerabilities
- Monitor and implement the further development of the technology, especially in the area of cybersecurity

Always keep technology and knowledge up to date.

Consideration of the risks posed by cyber attacks in the Threat and Risk Assessment (TRA)

Make an inventory of all software, hardware, and infrastructure devices, in order to identify risks to the location or organization. Incident response procedures must be incorporated into all IT and manufacturing processes. The choice of risk mitigation measures should be based on a cost-benefit analysis and classification of risks. This is followed by the introduction of cybersecurity rules and procedures and the training of personnel.

Living the concept

Technical solutions alone are not sufficient to effectively counter threats.

Cybersecurity must be part of the corporate culture and process landscape and must be internalized and lived by all employees.

Continuously monitoring the security situation

You have the following options to monitor the cybersecurity situation continuously:

- Setting anomaly references and creating allow and deny lists based on normal network communication and production machine behavior. The SINEC software family offers you reliable security tools (<https://www.siemens.com/global/en/products/automation/industrial-communication/sinec-network-software/cybersecurity.html>) to detect potential vulnerabilities in OT networks, quickly initiate suitable measures and resolve security vulnerabilities in a targeted manner.
- Establishment of an intrusion detection system (IDS) that generates alarms when unusual behavior occurs in the network
- Introduction of a Security Information and Event Management (SIEM) system to collect, analyze, and evaluate events in real time to enable early countermeasures
- Measures regarding network security: for example, network segmentation, firewalls, VPN, DMZ (demilitarized zones)

2.5 Operational application environment and security assumptions

2.5.1 Intended use

SIMATIC products are intended for use in industry. If you plan to use the product in a different environment, check the conditions required for such use.

The product may be operated only by personnel qualified for the specific task in accordance with the relevant documentation, in particular its warning notices and safety information. Qualified personnel are those who, based on their training and experience, are capable of identifying risks and avoiding potential hazards when working with these products.

Operational reliability and intended use

Before using your product, read the introductory information about operational guidelines and intended use. Also read the Technical Specifications for your components of your system.

2.5.2 Requirements for the operational application environment and security assumptions

Siemens recommends the following security measures:

- Threat and Risk Assessments (as part of security management)
- Network security concepts
 - Network segmentation
 - Asset and network management
 - Network protection
 - Remote access
- Access control concepts (utilizing access control systems)
 - Physical protection
 - Physical corporate security
 - Physical product security

Threat and Risk Assessment

Vulnerabilities and risks are identified, and countermeasures are proposed to ensure the security of the system, networks, and data.

Network security concepts

You can find information on network security in the whitepaper "Industrial Network Security Architecture", available at the Download Center (<https://www.siemens.com/us/en/company/topic-areas/cybersecurity/industrial-security/downloads.html>) on the Industrial Cybersecurity (<https://www.siemens.com/us/en/company/topic-areas/cybersecurity/industrial-security.html>) website.

Access control concepts

Physical protection

In addition to closing off and/or monitoring entire production facilities, it may be necessary to physically secure cabinets or even individual components such as circuit breakers.

Physical corporate security

You can ensure physical corporate security by the following measures, among others:

- Closed off and monitored company premises
- Access control, locks/card readers, and/or security personnel
- Accompaniment of non-employees by company personnel
- Employees are trained on and embrace security processes within the company

Physical production security

You can ensure the physical production security by, among others, the following measures:

- Separate access control for critical areas, such as production zones.
- Installation of critical components in lockable cabinets/control rooms with monitoring and alarm capabilities. The cabinets/control rooms must be secured with a cylinder lock. Do not use simple locks, such as universal, triangular/square, or double-bit locks.
- Radio field planning to limit WLAN coverage areas, preventing them from extending beyond defined zones (e.g. factory floor).
- Guidelines that prohibit the use of external data storage media (such as USB flash drives) and IT devices (such as laptops) classified as unsafe on systems.

2.6 Security properties of the devices

The security properties of the individual devices are listed in the Equipment Manuals.

2.7 Secure operation of the system

This section describes measures recommended by Siemens to protect your system from manipulation and unauthorized access.

2.7.1 Hardening measures

System hardening, also simply referred to as hardening, is the secure configuration of products or systems. The aim is to close security gaps and take various measures to reduce the attack surfaces for cyberattacks.

Measures for system hardening include, for example:

- Secure configuration in which only necessary software components and services are installed or activated for proper operation.
- Access control, by which a restrictive user and rights management system is implemented.

2.7.2 Secure configuration

Secure configuration involves control over all software components, along with their interfaces, ports, and services.

Activated services and ports pose a risk, for example of unauthorized access to the network and to programs.

To minimize the risk, activate solely the required services at all the automation components. Take all activated services (especially Web servers, FTP, remote maintenance etc.) into account in the security concept. Consider the default states of ports and services in your security concept.

You can find an overview of all ports and services used in the Communication Function Manual (<https://support.industry.siemens.com/cs/ww/en/view/59192925>).

2.7.3 Access control

In addition to physical protection, also establish logical safeguards to control access to your system:

- Use a restrictive user and rights management system, for example, for accessing the CPUs and TIA Portal.
- Refer to the information about password management in the section Protection (Page 185) and in the STEP 7 online help (TIA Portal).

See also

[Password management \(Page 37\)](#)

2.7.4 Handling of sensitive data

Data protection information

Siemens Aktiengesellschaft observes the applicable data protection laws, including the General Data Protection Regulation (GDPR), in particular the rules of data minimization and data-protection-friendly default settings (privacy by design, privacy by default).

This means for the products in this system:

Products with user management save user names and passwords to manage access rights. User names are also saved in logging alarms. These logging alarms are provided with a time stamp and stored in the internal cache of the CPU. They can be forwarded to a central syslog server. You can find more information in the section Syslog messages (Page 43).

In addition, the products do not store any personal data.

If you establish a reference to an identifiable person by linking these data with other data (such as shift schedules), or if you store personal data on the same medium (such as a hard disk), you must yourself ensure that the data protection regulations are observed.

Information on the secure removal of data from the CPU, interface module and SIMATIC Memory Card is provided in the section Secure decommissioning (Page 32).

Storage of security-relevant data

When storing your security-relevant data on your PC, independently ensure secure data storage.

Also observe the section Sensitive data (Page 40).

2.7.5 Regular firmware updates

NOTE

Outdated firmware versions might not be monitored for security vulnerabilities.

- Always keep your plant/products up to date to benefit from troubleshooting and to minimize potential risks.
 - Use email notifications to be automatically informed about firmware updates.
-

You can find more information in the following:

- The section Firmware update (<https://sieportal.siemens.com/su/blqEr>)
- The section Notification of security updates (Page 31)

2.7.6 Notifications about security vulnerabilities (Siemens Security Advisories)

A vulnerability is a security vulnerability in information security. A vulnerability can pose a threat as it provides intruders with the opportunity to access system resources and manipulate or steal data. Many vulnerabilities allow availability to be impaired.

Siemens ProductCERT

If Siemens identifies or fixes Security Vulnerabilities in the products, this will be published in the Security Advisories.

You can find the documents for SIMATIC on the following website of the Siemens Aktiengesellschaft: Siemens ProductCERT and Siemens CERT (<https://new.siemens.com/global/en/products/services/cert.html?s=SIMATIC#SecurityPublications>)

"Search Security Advisories" is the default entry in the "SIMATIC" search field. You can also enter other product names or other terms in the search field and search for them.

On this page, you will also find all the required information on how to deal with vulnerabilities:

- Contact persons for matters related to vulnerabilities
- Options for automated notifications regarding vulnerabilities
- Notifications are also possible in CSAF format
- Option to subscribe to RSS feeds and newsletters
- List of all current vulnerabilities and detailed information such as:
 - Description
 - Classification according to Common Vulnerability Scoring System (CVSS)
 - Measures
 - Availability
 - Etc.

Set up Security feeds (<https://www.siemens.com/cert>) to receive notifications about security-related topics.

If you suspect or have discovered a vulnerability in a Siemens product, please let us know immediately. To do this, press the "Contact" button on the CERT Services page (<https://www.siemens.com/cert>) and follow the instructions.

2.7.7 Data backup

Secure your configuration and parameter settings so that you can quickly restore this data if needed.

2.7.8 Security checks

Security checks for data, files, and archives serve to ensure data integrity at the storage location and during file transmission, protecting against manipulation and transmission errors. This is often achieved using digital checksums that are provided alongside the data. Tools (such as SHA-256 or SHA-512) for calculating and verifying these checksums are provided in many systems and named according to their respective calculation methods.

File Integrity Guidelines describe the prescribed procedure for integrity checks.

Integrity protection is a protection function for engineering data and firmware files.

Communication integrity means protecting communication against unauthorized manipulations to ensure high system availability. A central element in this regard is, for example, the use of digital checksums when accessing controllers. (Source: Industrial Cybersecurity website (<https://www.siemens.com/us/en/company/topic-areas/cybersecurity/industrial-security.html>))

2.7.9 Secure decommissioning

In the following section, you will find information on how to properly decommission individual components of your automation system. Decommissioning is necessary when the component has reached the end of its service life.

Decommissioning includes environmentally sound disposal and secure removal of all digital data of electronic components with storage medium.

2.7.9.1 Securely removing data

Before disposing of components of your automation system, you should securely delete all data from the storage media of these components. How to securely delete data from the devices so that it cannot be recovered is described below.

NOTICE
Data misuse resulting from non-secure deletion of data
Incomplete or non-secure deletion of data from data memories can result in data misuse by third parties.
For this reason, ensure secure deletion of data from all storage media used before disposing of the product.

Secure erasure of data from the CPU and SIMATIC Memory Card

To delete all data from the data memories of the CPU, reset the CPU to factory settings. The function deletes all information that was saved internally on the module.

For secure deletion of the data, follow these steps in the order given:

1. Format the SIMATIC Memory Card.

The formatting deletes all contents from the SIMATIC Memory Card.

Formatting with STEP 7:

- Establish an online connection.
- Open the online and diagnostics view of the CPU (either from the project context or via "Accessible devices").
- In the dialog window, select "Functions > Format memory card" and then click the "Format" button.

Formatting using the display of a CPU:

- In the display of the CPU, select the menu "Settings" > "Card functions" > "Format card" and confirm with OK.

2. Restore the factory settings of the CPU.

We recommend resetting the CPU in STEP 7. When you reset a CPU to factory settings, select the options shown in the figure before the reset.

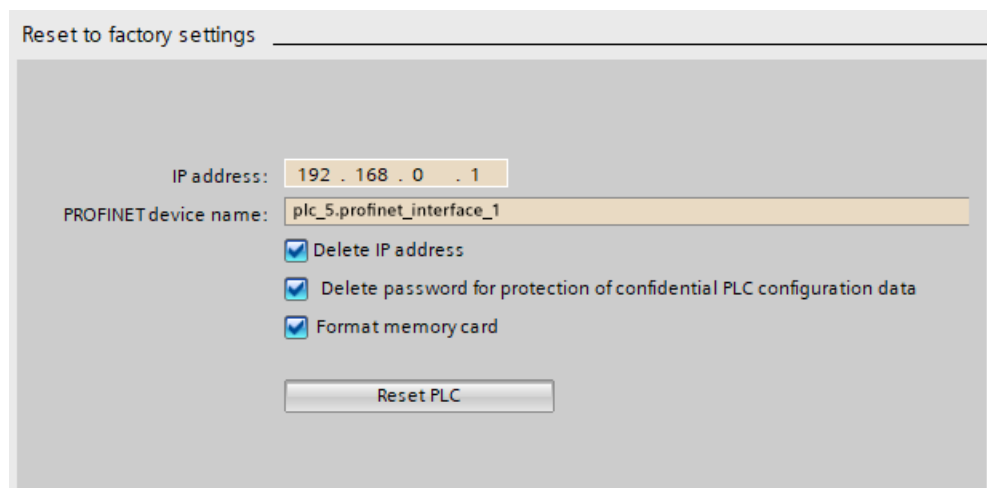


Figure 2-1 Resetting the CPU to factory settings

NOTE

If you reset the CPU using STEP 7 and you have selected the "Format memory card" option, you can skip step 1 of the described sequence of steps.

Result: All data that was still contained in the data memories of the modules and the SIMATIC Memory Card has been deleted. You can now dispose of the components.

For more information on resetting the CPU to factory settings, refer to the section Resetting the CPU to factory settings

(https://docs.tia.siemens.cloud/access?ft:originId=HWCDiagenUS_20.00.00.00_release&ft:clusterIdHWCDiag).

NOTE

If you no longer plan to use the SIMATIC Memory Card after formatting it, destroy it before disposing of it.

A secure destruction method is to shred the card to such a degree that it cannot be reconstructed. For this, you can also use a waste disposal service that specializes in data storage medium destruction.

Secure erasure of data from the interface module

With the following tools, you can securely erase the data from the interface module:

- STEP 7 < V19
- SIMATIC Automation Tool
- MultiFieldbus Configuration Tool (MFCT)
- PRONETA

Follow these steps in the order given:

1. Establish an online connection.
2. Open the Online and Diagnostics view of the IM (either from the project context or via "Accessible devices").
3. In the dialog box "Functions > Reset to factory settings", select the option "Delete I&M data" and then the "Reset" button.

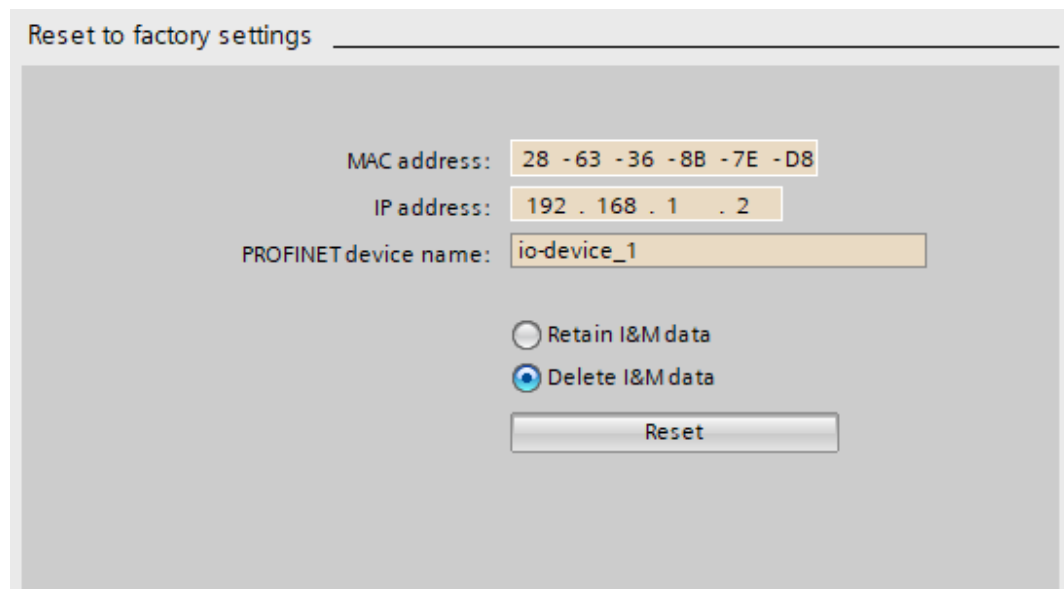


Figure 2-2 Resetting an interface module to factory settings

Result: All the data that was still in the data memories of the interface module was deleted. You can now dispose of the components.

For more information on resetting the interface module to factory settings, refer to the section [Resetting an interface module to factory settings](#)

(https://docs.tia.siemens.cloud/access?ft:originId=HWCDiagenUS_20.00.00.00_release&ft:clusterIdHWCDiag).

NOTE**STEP 7 ≥ V19**

Only the communication parameters will be securely deleted on "Reset to factory settings" with the "Delete I&M data" option enabled when you use STEP 7 ≥ V19.

Deleted communication parameters:

- IP address
- Device name
- PROFINET configuration data

If you want to securely remove all data, use one of the tools listed above for this purpose.

2.7.9.2 Recycling and disposal

For environmentally sustainable recycling and disposal of your old equipment, contact a certified electronic waste disposal service and dispose of the equipment according to the applicable regulations in your country.

NOTE**Recycler Guides**

Disassembly of electronic devices may only be carried out by specialists trained in the recycling of electronic products.

The Siemens Recycler Guides provide step-by-step disassembly instructions and material composition information of the products. This information helps recyclers direct specific materials to specialized recyclers and thus maximize the recovery of resources.

You can find the Recycler Guides in the SiePortal (<https://sieportal.siemens.com/en-ww/mysieportal>) in the "Support" area by using the search term "Recycler Guide".

2.8 Secure operation of the engineering software

For more information on secure operation of the engineering software, refer to the TIA Portal online help.

2.9 Secure operation of the CPUs

This section describes measures recommended by Siemens to protect your device from manipulation and unauthorized access.

2.9.1 Secure configuration

Information about ports, services, and default states can be found in the Communication Function Manual (<https://support.industry.siemens.com/cs/ww/en/view/59192925>) and the Equipment Manual.

2.9.2 User management and access control

2.9.2.1 Administration of user accounts

Creating and managing user accounts with appropriate usage rights is an important measure, as every active user represents a potential security risk.

Take the following security measures:

- Train your personnel in understanding their rights and password assignment
- Regularly check the user accounts

You can find information on creating and managing user accounts in the Protection (https://docs.tia.siemens.cloud/access?ft:originId=../100365717643/100365717643_enUS.htm&ft:clusterId/100365717643/100365717643.htm) section under "User management" and in the online help for STEP 7 (TIA Portal).

2.9.2.2 Assigning secure passwords

Using non-secure passwords can easily lead to data misuse. Non-secure passwords can be easily guessed or decrypted.

- Therefore, always change the default passwords during commissioning and use different passwords for different users, functions and devices.
- When changing the password, do not use passwords (or parts of passwords) that were used in the past.
- Also, change passwords for functions you don't personally use to prevent misuse of such unused functions.
- Always keep your passwords confidential and ensure that only authorized individuals have access to the respective passwords.
- Go over the required minimum password length and use a mixture of lower- and upper-case letters, numbers and characters.

The STEP 7 online help (TIA Portal) provides information on creating secure passwords.

Overview of all components and functions with password protection

Components and functions with password protection	Comment
SIMATIC S7 app	See section SIMATIC S7 app (https://www.siemens.com/global/en/products/software/mobile-apps/simatic2go.html)
Syslog (with certificate protection)	See section Syslog messages
CPU	See the Communication Function Manual (https://support.industry.siemens.com/cs/ww/en/view/59192925), section Secure Communication
OPC UA	See the Communication Function Manual (https://support.industry.siemens.com/cs/ww/en/view/59192925), section OPC UA communication
SNMP Community-String (similar to a password)	See the Communication Function Manual (https://support.industry.siemens.com/cs/ww/en/view/59192925), section SNMP
Secure communication (with certificate protection)	See the Communication Function Manual (https://support.industry.siemens.com/cs/ww/en/view/59192925), section Secure Communication
Web server	See the Web server Function Manual (https://support.industry.siemens.com/cs/ww/en/view/109977246)

2.9.2.3 Password management

- You can find comprehensive recommendations for creating secure passwords in the Industrial security Configuration Manual (<https://support.industry.siemens.com/cs/us/en/view/109974047>).
- Establish guidelines for assigning passwords and intervals for password changes.
- Settings for checking password policies when passwords are assigned or changed can be configured in the TIA Portal. For more information, please refer to the Communication Function Manual (<https://support.industry.siemens.com/cs/ww/en/view/59192925>).
- Modify and reset the password for protecting confidential configuration data.
You can find information on the following topics in the Communication Function Manual (<https://support.industry.siemens.com/cs/ww/en/view/59192925>):
 - Description of how to change the password
 - Description of how to delete or reset the password
 - Description of how to assign the password via a SIMATIC Memory Card
- Access to a password-protected CPU can be configured through the display, if the CPU has a display; see section Using the display to set additional password protection.

- For user management and access control, use the Local/central user management (https://docs.tia.siemens.cloud/access?ft:originId=./100365717643/100365717643_enUS.htm&ft:clusterId./100365717643/100365717643.htm).
- Using a password provider: In STEP 7, you can set up a password provider; see section Know-how protection (https://docs.tia.siemens.cloud/access?ft:originId=ProgBlockProtectionenUS_20.00.00.00_release&ft:clusterIdProgBlockProtection).
- In addition, you can use commercially available password management programs.

Setting password protection without engineering system

You can change your password for a user account in the user management via the web server of the CPU:

- API method Api.ChangePassword: Changing a password in runtime

You can find more information about the available methods of the web server's Web API in the Web server (<https://support.industry.siemens.com/cs/ww/en/view/109977246>) Function Manual.

2.9.2.4 Setting protection levels

For detailed information about setting up protection levels for the CPU and assigning user authorizations, refer to the section Configuring access protection for the CPU (https://docs.tia.siemens.cloud/access?ft:originId=./11627607179/171587178635_enUS.htm&ft:clusterId./11627607179/171587178635.htm) and the STEP 7 online help (TIA Portal).

2.9.2.5 Certificate management

You can create, assign and manage certificates with TIA Portal for the following functions of the CPUs:

- Secure Open User Communication
- OPC UA communication
- Secure PG/HMI communication
- Web server

You can find all relevant information about "Certificate management" in the Communication Function Manual (<https://support.industry.siemens.com/cs/ww/en/view/59192925>).

2.9.3 Protection functions

Integrated protection functions of the CPU protect against unauthorized access.

You can find an overview of the protective functions supported by your CPU in the respective Equipment Manual.

A description of the protection functions and their activation can be found in the section Protection (https://docs.tia.siemens.cloud/access?ft:originId=ProgCPU15enUS_20.00.00.00_release&ft:clusterIdProgCPU15).

2.9.4 Signed firmware update for CPUs

Signed firmware update

A signed firmware update ensures the authenticity and integrity of the firmware loaded onto a device.

It protects you against installing malicious firmware in case:

- Firmware was modified
- Firmware was downloaded from an incorrect Internet source

Principle of the signed firmware updates for CPUs

Firmware updates for CPUs contain a digital signature.

The digitally signed firmware update files are available for download on the Siemens Support Web page (<https://sieportal.siemens.com/su/blqEr>).

The CPU verifies the authenticity and integrity of the firmware update file before installation using the digital signature with standardized asymmetric cryptography methods. As a result, the CPU can detect a manipulated or corrupted firmware update file and reject it.

Note that the CPU performs the verification only after the complete firmware download has taken place.

The procedure for carrying out firmware updates for CPUs is described in the section Firmware update (<https://support.industry.siemens.com/cs/ww/en/view/109988293/185156409355>).

Diagnostics alarms and remedy

The success/failure of the signed firmware update is reported:

- In the diagnostics buffer of the CPU
- On the display of the CPU if the CPU has a display
- In the Syslog storage of the CPU

In case of firmware update rejection, proceed as follows:

1. Check whether the firmware update file used by you originates from a secure source and was downloaded unchanged. As a check calculate the hash value of the downloaded firmware update file and compare it with the value specified on the download page.
2. Download the firmware again from the Siemens Support Web page.
3. Repeat the firmware update.

Information on the procedure for calculating and comparing hash values is available on the Internet (<https://support.industry.siemens.com/cs/ww/en/view/109483101>).

2.9.5 Secure Boot for CPUs

Secure Boot

Secure Boot verifies, before the boot process, whether firmware has been falsified, for example through manipulation or accidental falsification.

Secure Boot ensures the authenticity and integrity of the firmware executed by the device.

Principle of "Secure Boot" for CPUs

CPUs verify the authenticity and integrity of the firmware to be executed using "Secure Boot" before their startup.

The verification is carried out using standardized asymmetric cryptography methods.

In addition to the signed firmware update for CPUs (Page 39), Secure Boot prevents a manipulation of the firmware by a physical intervention into the CPU.

Secure Boot is integrated in the CPU and cannot be deactivated for security reasons.

2.9.6 Secure communication/OPC UA

Additional protection is provided by the protection functions of the secure communication and OPC UA protocols.

Information about the protocols Secure Communication and OPC UA can be found in the Communication Function Manual

(<https://support.industry.siemens.com/cs/ww/en/view/59192925>).

2.9.7 Sensitive data

Security-relevant and sensitive data can be protected through appropriate measures such as passwords and protection functions.

For certain data, protection is already essential and implemented within the system (e.g. certificate management in the TIA Portal).

Sensitive data	Comment	Where can I find more information?
Confidential configuration data (private keys, passwords/access data)	Protection by using a strong password	Communication Function Manual (https://support.industry.siemens.com/cs/ww/en/view/59192925), section Protection of confidential configuration data
User management data	-	Protection (https://docs.tia.siemens.cloud/access?ft:originId=ProgCPU15enUS_20.00.00.00_release&ft:clusterIdProgCPU15) section STEP 7 online help

Sensitive data	Comment	Where can I find more information?
Configuration of CPUs and interface modules	Protection through PROFINET Security Class 1	Function manual PROFINET with STEP 7 (https://support.industry.siemens.com/cs/ww/en/view/49948856)
Blocks (data blocks, logic blocks)	Know-how protection, copy protection, write protection	Protection (https://docs.tia.siemens.cloud/access?ft:originId=ProgBlockProtectionenUS_20.00.00.00_release&ft:clusterIdProgBlockProtection) section
Data deemed sensitive by the operator	Backups, other configuration data, analysis data	Backing up and restoring the CPU configuration (https://docs.tia.siemens.cloud/access?ft:originId=ProgOnlineBackupenUS_20.00.00.00_release&ft:clusterIdProgOnlineBackup) section

2.9.8 Backups and data backups

Regular data backups after successful installation should be part of a successful security concept. Whether for restoring a project if required, if the changes made do not yield the desired results, or for saving an installation in an emergency.

Backup of a STEP 7 project:

- Project backup via the SIMATIC Automation Tool
- Project backup via TIA Portal, see FAQ What options are there in STEP 7 (TIA Portal) for backing up projects and what is the significance of the backup files of the projects?
(<https://support.industry.siemens.com/cs/us/en/view/92561565>)

You can find more information in the section Backing up and restoring the CPU configuration
(https://docs.tia.siemens.cloud/access?ft:originId=ProgOnlineBackupenUS_20.00.00.00_release&ft:clusterIdProgOnlineBackup).

2.9.9 Additional protective measures for network security

In addition to the protective measures described in this manual, you can find information on network security and network components for protection against unauthorized access in the Network security section of the PROFINET Function Manual
(<https://support.industry.siemens.com/cs/ww/en/view/49948856>).

See also

SIMATIC CP 1243-1 (<https://sieportal.siemens.com/su/blYx6>)

2.9.10 Using a Web server

The CPUs have an integrated Web server.
It comes with built-in security features:

- Activation for specific interfaces
- Access via the secure transmission protocol "HTTPS" using the CA-signed or self-signed web server certificate
- Authentication via local or central user management
- Changing the password of local users during runtime using Web-API

When using Web servers, traditional firewalls are no longer sufficient to protect modern networks.

Information about potential risks when using Web servers can be found in the Web server Function Manual (<https://support.industry.siemens.com/cs/ww/en/view/109977246>).

2.9.11 Recording security events

Syslog storage

Syslog stands for "System Logging Protocol," a standard for transmitting log messages triggered by security events. Predefined events in a network device are collected as security events in the device (syslog client) and stored as syslog messages in the local cache.

A syslog server collects and categorizes syslog messages, which can then be analyzed and filtered and displayed in various ways. Additionally, notifications for critical events can be configured.

The following security events, for example, are collected in the CPU diagnostic buffer:

- Going online with the correct or incorrect password
- Manipulated communication data detected
- Manipulated data detected on memory card
- Manipulated firmware update file detected
- Changed protection level (access protection) downloaded to the CPU
- Password legitimization restricted or enabled (via an instruction or, if applicable, the CPU display)
- Online access denied due to the possible number of simultaneous access attempts being exceeded
- Timeout when an existing online connection is inactive
- Logging on to the Web server with the correct or incorrect password
- Creating a backup of the CPU
- Restoring the CPU configuration (Restore)

The security events listed above are also stored as syslog messages in the local cache of a CPU. You can find an overview of all syslog messages in the following Entry (<https://support.industry.siemens.com/cs/ww/en/view/109823696>).

The content of a syslog message is based on IEC 62443-3-3.

You can find more information in the section Syslog messages ([Page 43](#)).

Connection to a SIEM system

A SIEM system (Security Information and Event Management) analyzes security events in real time and can be installed, for example, on the syslog server.

2.9.12 Syslog messages

Using syslog messages

International standards and national regulations for the IT security of automation components require, for example, the ability to log safety-related events.

Syslog (System Logging) is an IETF standard protocol (RFC 5424) for the transfer of recorded events and meets this requirement. A CPU records the following events, for example:

- Security events
- Firmware updates
- Changes to the user program
- Changes to the configuration
- Changes to the operating mode

The collecting of security-relevant events cannot be deactivated. Each CPU saves syslog messages in a local cache. By querying this cache, you can view the syslog messages and identify potential security risks.

The cache of a CPU is organized as a ring buffer. If the storage limit of the cache is reached and additional security events occur, the oldest messages in the cache are overwritten.

You have the option of transferring the events collected by the CPU to a syslog server in the network.

Forwarding to a syslog server

You can transfer syslog messages to a server, for example, SINEC INS. The syslog messages are transferred to the syslog server via the syslog protocol. The syslog server saves all syslog messages from its connected devices. Messages of system and network events are stored centrally in a storage location in the syslog server. At the syslog server interface, you can view the collected syslog messages and thereby determine the source of potential security risks or problems.

Syslog messages are sent to the syslog server via port 514 (UDP) or port 6514 (TLS over TCP) by default.

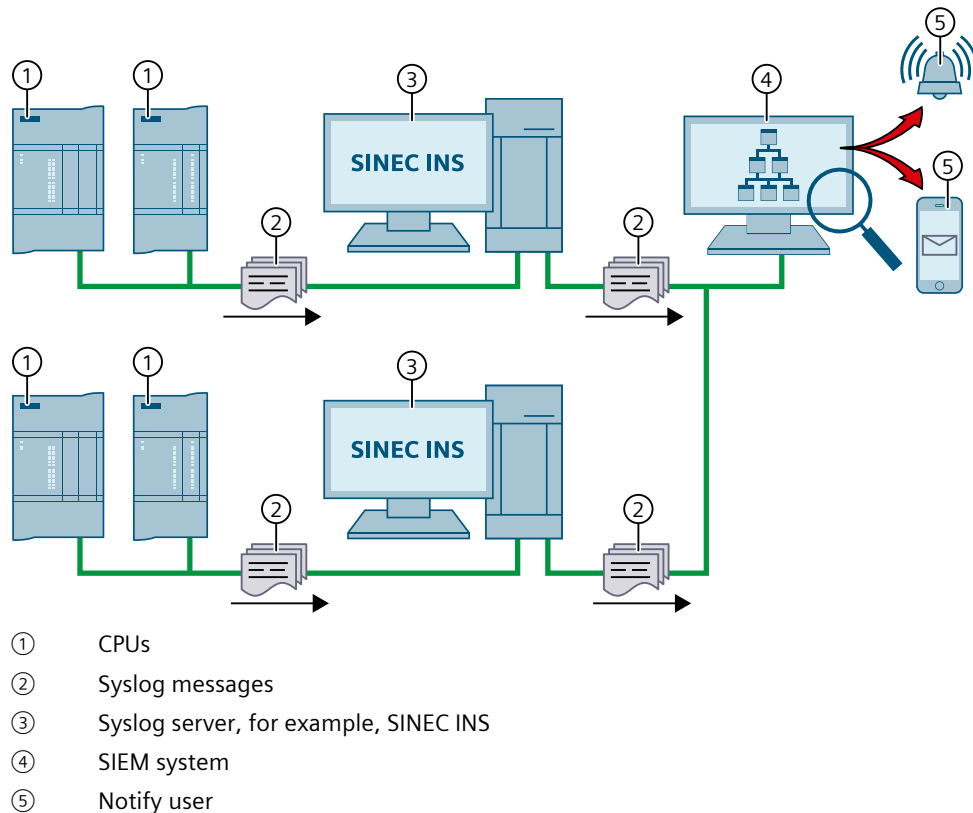
NOTE

If you are using UDP as the transport protocol, the data is transmitted unencrypted. Authentication is also omitted with UDP.

Processing in a Security Information and Event Management system (SIEM system)

In order to be able to accept and process the incoming syslog messages, a SIEM system must "understand" the syslog protocol according to RFC 5424.

The SIEM system breaks down the incoming syslog messages into individual elements. These elements are assigned to their own event within the SIEM system. Within this event, it is analyzed whether there are connections between the individual syslog messages. In this way, the SIEM system detects possible attack vectors and, if necessary, informs the user, e.g. in the event of multiple attacks at several points in the system.



More information

More information on network management with SINEC INS is available in the "SIMATIC NET: Network management SINEC INS V1.0 SP2

(<https://support.industry.siemens.com/cs/us/en/view/109781023>)" manual.

You can find information on the structure of syslog messages in the Structure of the Syslog messages (Page 48) section.

2.9.12.1 Transfer of the syslog messages to a syslog server

A CPU can send syslog messages to a syslog server via a TLS or UDP connection.

Recommendation: Use solely a TLS connection for the productive operation. You can also use a UDP connection for commissioning or testing scenarios.

Transmitting syslog messages via a TLS connection

A TLS connection ensures that all syslog messages from a CPU are securely transmitted to the syslog server. If the TLS connection is interrupted, the syslog messages are cached in the CPU cache. The CPU only sends the cached syslog messages when the TLS connection to the syslog server is established again.

Each syslog message is transferred to a syslog server only once. If you address another syslog server in the settings for the syslog server, syslog messages that have already been transferred are not transferred to a newly configured syslog server.

Since the cache of a CPU is organized as a ring buffer, the oldest messages are overwritten as soon as the memory limit is reached and further security events occur. Overwriting syslog messages that have not yet been transferred to a syslog server is reported as a security event (overflow event) in syslog storage. If syslog messages are overwritten over a long period of time, the overflow event is repeated regularly. As soon as the first message is sent back to the syslog server, another security event is generated. This security event confirms that syslog messages are being transferred back to the syslog server.

Message in the diagnostics buffer of the CPU

If a syslog server is configured in the CPU properties, the CPU also records overwriting of non-transmitted syslog messages in the diagnostics buffer.

As soon as a non-transmitted syslog message is overwritten, the CPU reports maintenance demanded as an incoming event in the diagnostics buffer. In addition, the MAINT LED of the CPU also signals incoming maintenance demanded.

As soon as the syslog messages are sent back to the syslog server, the CPU reports maintenance demanded as an outgoing event in the diagnostics buffer. If the CPU does not report any further maintenance demanded, the MAINT LED also turns off again.

Information on the status and error display of the CPU can be found in the respective device manuals.

Requirements

If you want to transfer the syslog messages of a CPU to a syslog server, the following requirements must be met:

- STEP 7 as of version V20
- S7-1200 G2 CPU as of FW version V1.0
- A project has been created in STEP 7
- The device or network view of STEP 7 is open

Procedure

To configure the CPU to transfer syslog messages to a syslog server, follow these steps:

1. Select the required CPU in the device or network view of STEP 7.
2. In the Inspector window, navigate to "Properties > Protection & Security > Syslog > Syslog server".
3. In the "Connection to syslog server" area, select the "Enable transfer of syslog messages to a syslog server" option. The selection options below become editable.
4. Select one of the following options from the "Transport protocol" drop-down list:
 - "Transport Layer Security (TLS) - server and client authentication": Encrypted data transfer, syslog server and client (CPU) must authenticate themselves.
 - "Transport Layer Security (TLS) - only server authentication": Encrypted data transfer, only the syslog server needs to authenticate itself.
 - "UDP": Unencrypted data transfer, syslog server and client (CPU) do not need to authenticate themselves.

In the next sections you can read how to select the certificates for authentication (logon) depending on the settings specified.

5. In the "Addresses of the syslog servers" column, enter a valid server address.
6. In the "Port" column, enter a valid port number.
By default, STEP 7 uses the following port numbers:
 - Standard TCP port for TLS: 6514
 - Standard UDP port: 514

Result: You have configured the transfer of syslog messages to a syslog server.

> Syslog server

Connection to syslog server (max. 1)

☒ Enable transfer of syslog messages to a syslog server

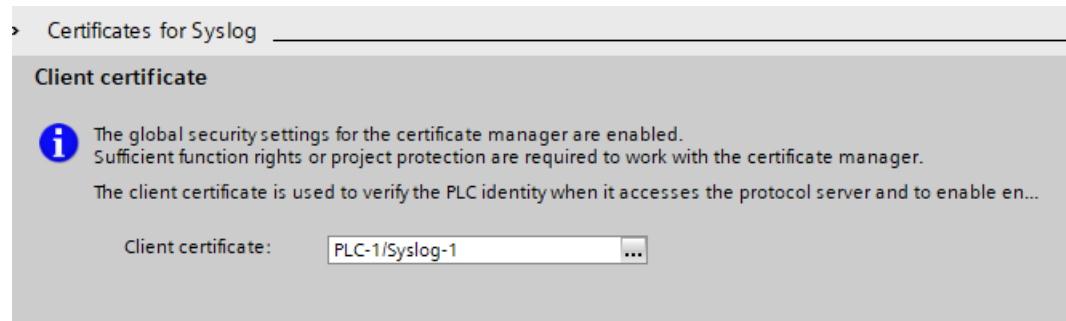
Transport protocol: Transport Layer Security (TLS) - server and client authentication

Addresses of the syslog servers	Port
192.168.0.100	6514
<Add new server>	

Selecting the client certificate

STEP 7 provides the required client certificate for a CPU for the TLS transport protocol. If the certificate is managed within the CPU, you can either choose an existing certificate or create a new certificate. To do so, follow these steps:

1. Select the required CPU in the device or network view of STEP 7.
2. In the Inspector window, navigate to "Properties > Protection & Security > Syslog > Certificates for Syslog".
3. Select the appropriate certificate in the "Client certificate" field.



Selecting the server authentication

After selecting the TLS transport protocol, the configured syslog server must authenticate itself. This ensures that the CPU only connects to a trusted server. If you want to waive server authentication, activate the automatic acceptance of server certificates during runtime. To configure these settings, follow these steps:

1. Select the required CPU in the device or network view of STEP 7.
2. In the Inspector window, navigate to "Properties > Protection & Security > Syslog > Certificates for Syslog".
3. In the "Trusted servers" area, specify whether the connected syslog server is to be authenticated. In this case, it is necessary to complete the following information:
 - Add trusted server: Add a valid server certificate in the "Common name of subject" column.
 - Automatically accept certificates during runtime: Activate the "Automatically accept server certificates during runtime" option. Editing in the table is then not possible.

NOTE

No authentication with automatically accepted server certificates

If you enable the "Automatically accept server certificates during runtime" option, a server does not need to authenticate itself. This means that the CPU can also connect to unknown servers that could represent a security risk.

Only select this option during commissioning or in a protected environment.

2.9.12.2 Structure of the Syslog messages

A CPU collects syslog messages in a local cache. These syslog messages are structured according to the syslog protocol (RFC 5424) and consist of the following elements:

- HEADER
- STRUCTURED-DATA
- MSG (Message)

The following sections describe the structure and parameters of the individual elements.

Structure of the HEADER element

The header contains all the data required for further processing of the syslog message. A space separates the individual parts of the header (exception: No space between PRI and VERSION). A CPU transmits the following header in syslog messages, for example:

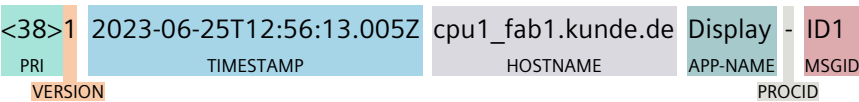


Figure 2-3 Example: HEADER of the syslog message of a CPU

The following table describes the parameters in the prescribed order.

Parameter	Description
PRI	PRI encodes the priority of the syslog message, divided into Severity (severity of the message) and Facility (origin of the message). The PRI value is formed as follows: • $PRI = Facility \times 8 + Severity$ Possible values: • Severity – 0 = Emergency: system is unusable – 1 = Alert: action must be taken immediately – 2 = Critical: critical conditions – 3 = Error: error conditions – 4 = Warning: warning conditions – 5 = Notice: normal but significant condition – 6 = Informational: informational messages – 7 = Debug: debug-level messages • Facility – 1 = User-level messages – 2 = Mail system – 3 = System daemons – 4 = Security/authorization messages – 5 = Messages generated internally by syslog – 6 = Line printer subsystem – 7 = Network news subsystem – 8 = UUCP subsystem – 9 = Clock daemon – 10 = Security/authorization messages – 11 = FTP daemon – 12 = NTP subsystem – 13 = Log audit – 14 = Log alert

Parameter	Description
	A CPU does not use all of the listed severity/facility values.
VERSION	Version number of the syslog specification.
TIMESTAMP	The device sends the time stamp in the format "2023-06-25T12:56:13.005Z" as UTC time without time zone and correction for daylight-saving/standard time.
HOSTNAME	Contains the name or the IP address (PROFINET interface X1) of the device or system from which the syslog message has been sent. IPv4 address according to RFC1035: Bytes in decimal representation: XXX.XXX.XXX.XXX IPv6 address according to RFC4291 Section 2.2 "-" is output if information is missing.
APP-NAME	Contains the component (device part or application) from which the message has been generated. "-" is output if information is missing.
PROCID	The process ID serves to clearly identify the individual processes, for example during analysis and troubleshooting. "-" is output if information is missing.
MSGID	ID to identify the message. "-" is output if information is missing.

Structure of the STRUCTURED-DATA element

STRUCTURED-DATA provides information in an interpretable and decomposable data format. The following applications are possible, for example:

- More information about the syslog message
- Application specific information

STRUCTURED-DATA can contain one or more elements (SD-ELEMENT). Each SD element must be enclosed in square brackets. If STRUCTURED-DATA consists of multiple SD elements, the individual SD elements are separated by a space.

Each SD-ELEMENT consists of its name (SD-ID) and one or more name-value pairs (SD-PARAM). Each name-value pair consists of a parameter name (PARAM-NAME) and the associated value (PARAM-VALUE). A space separates the individual components (SD-ID and SD-PARAM) within an SD element.

A CPU transmits the following SD ELEMENT in a syslog message, for example:

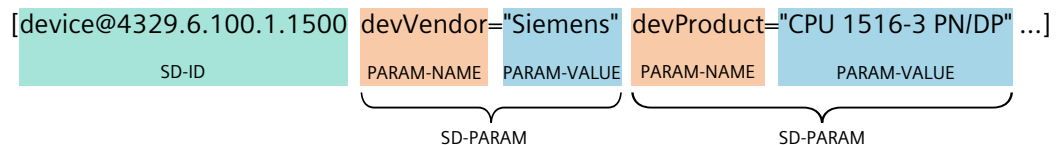


Figure 2-4 Example: SD ELEMENT of the syslog message of a CPU

Structure of the MSG element

In the MSG (MESSAGE) element, a CPU transmits the simplified name of the event in English. The following table shows what the content of a message of the MESSAGE element can look like.

MESSAGE	Description
SE_LOCAL_SUCCESSFUL_LOGON	The local logon has been successful (e.g. on the operator display of the CPU).

More information

You can read more information about the structure and transmission of syslog messages in the following RFCs (Request for Comments):

- The syslog protocol (RFC 5424) (<https://tools.ietf.org/html/rfc5424>)
- Transferring syslog messages via Transport Layer Security (RFC 5425) (<https://tools.ietf.org/html/rfc5425>)
- Transferring syslog messages via UDP (RFC 5426) (<https://tools.ietf.org/html/rfc5426>)

2.10 Secure operation of interface modules

Device-specific security information and instructions for interface modules can be found in the respective Equipment Manual.

2.10.1 Data integrity for interface modules

Data integrity refers to the completeness and correctness (integrity) of data, which is an essential prerequisite for the proper functioning of systems.

Measures for data privacy, data consistency, and data security ensure that data used within devices cannot be damaged, altered (manipulated), or deleted during processing or transmission, and at the very least, any changes to the data are detected.

Data integrity for interface modules

To detect intentional or accidental changes to data within an interface module and its associated modules, the possibility of dynamic integrity checking is introduced for PROFINET interface modules.

The ability to detect integrity breaches enhances the resilience of the distributed I/O system.

Data integrity within a distributed I/O system is entirely covered within the interface module and does not pertain to other components of the automation system.

Principle

The interface module calculates checksums based on its used data and the supplied data from the associated modules, such as parameter settings, IP address, device name, MAC address and I&M data. The interface module stores the checksums in the I&M4 data area.

A CRC (Cyclic Redundancy Check) is always the same for specific, unchanged memory content. When the memory content changes, the interface module (IM) calculates a different checksum for this content by reading and comparing the I&M4 data. By comparing with the initial CRC, you can determine whether the data in the memory has been modified or not:

- CRC stayed the same: No change in the data within this memory area of the interface module IM
- CRC changed: The data within this memory area of the IM was modified

Only you, as the user, know whether changes to the data of an interface module were intentional or not. If changes were not intentional, you can detect that the data of the interface module has been compromised through changed CRCs and respond accordingly.

I&M data

PROFINET devices provide Identification and Maintenance data (I&M data), which is a set of predefined data structures containing the internal module status. With this data, a module can be identified, its serial number can be determined, etc.

The CRC checksums are mapped in the maintenance data **I&M4** of the interface module.

NOTE

Requirements for calculating the CRCs

The CRCs via the memory contents of the interface module are calculated only when you request to read the I&M4 data.

The CRCs cover not only the interface module itself but can also take into consideration combined checksums from associated modules (refer to the section on the structure of the data record for I&M data). Process data is not included in the calculation of CRCs.

Example:

- You put your distributed I/O system into operation and read the CRC CHK_OVERALL with the value "0x55AAA678" ("16#55AAA678") from the interface module via the I&M4 data.
- As long as no changes have been made to the data of the interface module or the associated modules, each subsequent read will give the value "0x55AAA678" or "16#55AAA678".
- Once you read a different CRC CHK_OVERALL, for example, "0xCC9876FF", you will realize that there must have been changes to the data of the interface module or the associated modules.

The quality of the statement regarding the data integrity of the distributed I/O system improves with each module associated with the interface module that supports I&M4 data. Refer to the Equipment Manual of the respective module to find out if and from which firmware version the module supports I&M4 data.

The structure of the I&M data 0 to 4 is described in the section Record structure for I&M data (https://docs.tia.siemens.cloud/access?ft:prettyUrl=simatic_s7_1500_et_200mp_manual_collection_enus_20/basic-

[information/simatic-drive-controller/commissioning/identification-and-maintenance-data/record-structure-for-i-m-data](#)).

Spare parts scenario

The spare parts scenario is ensured. This means that you can replace interface modules with the same article number. For the "new" interface module, the static data such as the serial number and MAC addresses will change. Note that this is why the replacement is reflected in the changed identification data CHK_STATIC_LOCAL and consequently also in CHK_OVERALL.

More information on the spare parts scenario and compatibility can be found in the Equipment Manual of the interface module.

2.10.2 Signed firmware update for interface modules

Signed firmware update

A signed firmware update ensures the authenticity and integrity of the firmware loaded onto a device.

It protects you against installing malicious firmware in case:

- Firmware was modified
- Firmware was downloaded from an incorrect Internet source

Information on whether your interface module supports signed firmware updates is available in the Technical specifications section of the corresponding Equipment Manual.

Principle of the signed firmware update for interface modules

Firmware updates for interface modules may include a digital signature. The digitally signed firmware update files are available for download on the Siemens Support Web page.

The interface module verifies the authenticity and integrity of the firmware update file before installation using the digital signature with standardized asymmetric cryptography methods. As a result, the interface module can detect a manipulated or corrupted firmware update file and reject it.

Note that the interface module performs the verification only after the complete firmware download has taken place.

Subsequently, a notification is sent to the firmware update tool regarding the success or failure of the signature verification.

You still have all the options for firmware updates, as described in the Firmware update (https://docs.tia.siemens.cloud/access?ft:originId=HWCDiagenUS_20.00.00.00_release&ft:clusterIdHWCDiag) section, when performing signed firmware updates for modules. If the firmware update was not successful, the module will continue to run with the previous firmware.

Diagnostics alarms and remedy

When performing a firmware update for a module with an established connection between the IM and CPU, the following options for notifications are available in the CPU's diagnostic buffer:

- Successful integrity check of the firmware for the module
- Rejection of non-secure firmware for the module

You can find more information in the section on diagnostics alarms in the equipment manual for the respective module.

In case of firmware update rejection, proceed as follows:

1. Check whether the firmware update file used by you originates from a secure source and was downloaded unchanged. As a check calculate the hash value of the downloaded firmware update file and compare it with the value specified on the download page.
2. Download the firmware again from the Siemens Support website.
3. Repeat the firmware update.

Information on the procedure for calculating and comparing hash values is available on the Internet (<https://support.industry.siemens.com/cs/ww/en/view/109483101>).

2.10.3 Secure Boot for interface modules

Secure Boot

Secure Boot verifies, before the boot process, whether firmware has been falsified, for example through manipulation or accidental falsification. Secure Boot ensures the authenticity and integrity of the firmware executed by the device.

Information on whether your interface module supports Secure Boot is available in the Technical specifications section of the corresponding Equipment Manual.

Principle of "Secure Boot" for interface modules

Interface modules verify the authenticity and integrity of the firmware to be executed using "Secure Boot" before being executed.

The verification is carried out using standardized asymmetric cryptography methods.

In addition to signed firmware updates for interface modules, Secure Boot also prevents manipulation of the firmware through physical intervention in the interface module.

Secure Boot is integrated into the interface module and cannot be deactivated for security reasons.

NOTE

Longer startup duration of the interface module

The signature verification of Secure Boot significantly extends the startup time of the interface module. You can find time specifications in the Equipment Manual of the interface module, in the Technical specifications section.

LED display on the interface module

If the Secure Boot verification results in an invalid signature, the LEDs RUN, ERROR, and MAINT on the interface module will flash. In this case, you need to replace the interface module.

2.11 Secure operation of I/O modules

Device-specific security information and instructions for I/O modules can be found in the respective Equipment Manual.

2.11.1 Data integrity for I/O modules

Data integrity for I/O modules

In order to detect intentional or accidental changes to the data of an interface module and the assigned modules, the dynamic integrity check for I/O modules is introduced. Information on whether your I/O module supports the data integrity check is available in the Technical specifications section of the corresponding Equipment Manual.

Principle

The interface module calculates checksums based on its used data and the supplied data from the associated modules, such as serial numbers, parameter settings, calibration data and I&M data of I/O modules. The interface module stores the checksums in the I&M4 data area.

You can find more information on the principle of data integrity and I&M4 data in the section Data integrity for interface modules ([Page 50](#)).

Spare parts scenario

The spare parts scenario is still ensured. This means that you can replace I/O modules with the same article number. For the "new" I/O module, the static data such as the serial number will change. Note that the replacement is therefore reflected in the following modified I&M4 data of the interface module:

- CHK_STATIC_SUBS
- CHK_OVERALL_SUBS
- CHK_OVERALL

You can find the structure of I&M data in the section Record structure for I&M data

(https://docs.tia.siemens.cloud/r/simatic_s7_1500_et_200mp_manual_collection_enus_20/basic-information/simatic-drive-controller/commissioning/identification-and-maintenance-data/record-structure-for-i-m-data).

2.11.2 Signed firmware update for I/O modules

Signed firmware update

A signed firmware update ensures the authenticity and integrity of the firmware loaded onto a device.

It protects you against installing malicious firmware in case:

- Firmware was modified
- Firmware was downloaded from an incorrect Internet source

Signed firmware update for I/O modules

Firmware updates for I/O modules can contain a digital signature. Information on whether your I/O module supports signed firmware updates is available in the Technical specifications section of the corresponding Equipment Manual.

The digitally signed firmware update files are available for download on the Siemens Support Web page.

Principle, diagnostics alarms, and remedies

The principle and diagnostics of the signed firmware update are the same for interface modules and I/O modules. The information in the section Signed firmware update for interface modules [\(Page 52\)](#) applies.

2.12 Secure operation of power supply modules

Device-specific security information and instructions for the power supply modules can be found in the respective Equipment Manual.

2.12.1 Signed firmware update for system power supplies (PS)

Signed firmware update

A signed firmware update ensures the authenticity and integrity of the firmware loaded onto a device.

It protects you against installing malicious firmware in case:

- Firmware was modified
- Firmware was downloaded from an incorrect Internet source

Signed firmware update for system power supplies (PS)

Firmware updates for system power supplies (PS) can contain a digital signature. Information on whether your power supply module supports signed firmware updates is available in the Technical specifications section of the corresponding Equipment Manual.

The digitally signed firmware update files are available for download on the Siemens Support Web page.

Principle, diagnostics alarms, and remedies

The principle and diagnostics of the signed firmware update are the same for interface modules and I/O modules. The information in the section Signed firmware update for interface modules ([Page 52](#)) applies.

Product overview

3.1 Introducing the S7-1200 G2 PLC

The S7-1200 G2 PLC family is Generation 2 of the S7-1200 and offers a significantly narrower footprint than the first generation. The CPU and devices provide the flexibility and power to control a wide variety of automation applications. The configuration and programming software is STEP 7 within the TIA Portal framework. If you have used the STEP 7 configuration and programming software [\(Page 97\)](#) with other CPU families, take note of compatibility information [\(Page 177\)](#).

The CPU combines the following elements and more in a compact housing to create a powerful controller:

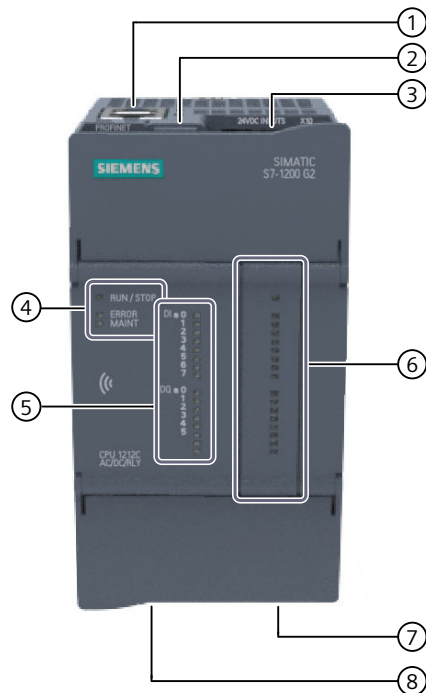
- A microprocessor
- An integrated power supply
- Input and output circuits
- Built-in PROFINET
- High-speed counters
- Standard and Advanced Motion Control

The S7-1200 G2 firmware adds new functionality and supports most of the previous S7-1200 functionality, with noted differences. [\(Page 61\)](#)

After you download your program, the CPU contains the logic required to monitor and control the devices in your application. The CPU monitors the inputs and changes the outputs according to the logic of your user program, which can include Boolean logic, counting, timing, complex math operations, motion control, and communications with other intelligent devices.

3.1 Introducing the S7-1200 G2 PLC

The CPU provides a built-in PROFINET interface with two ports for communication over a PROFINET network. You can connect additional Input, Output, and Communication modules [\(Page 59\)](#) to support larger automation applications.



- ① PROFINET interface with two ports, X1 (on the top of the CPU)
- ② Memory card slot, X50 (behind the door)
- ③ Removable input connector, X10 (behind the door)
- ④ Status LEDs for the CPU
- ⑤ Status LEDs for the on-board I/O
- ⑥ Optional plug-in expansion board, X300 (for CPUs with two slots, X300 and X301)
- ⑦ Removable output connector, X11 (behind the door, on the bottom of the CPU)
- ⑧ Power connector, X80 (behind the door, on the bottom of the CPU)

Several security features help protect access to both the CPU and the control program:

- Password protection that allows you to configure access to the CPU functions.
- "know-how protection" to hide the code within a specific block.
- Protection of confidential PLC configuration data
- Secure PG/PC and HMI communication
- Secure boot

You configure these security features in STEP 7. The TIA Portal Information System describes the types of security configurations.

For detailed information about a specific CPU or device, see the technical specifications [\(Page 356\)](#).

3.2 S7-1200 G2 modules and boards

You can connect expansion boards and expansion modules to the CPU to increase its functionality. The following types are available: Communication boards (CBs), Signal boards (SBs), Battery boards (BBs), Communication modules (CMs), Communication processors (CPs), and Signal modules (SMs).

Expansion boards

A variety of plug-in expansion boards are available for use with the S7-1200 G2 system:

- Communication boards (CBs)
- Signal boards (SBs)
- Battery boards (BBs)

You can add CBs, such as the RS485, to increase the communication capability of a CPU.

You can add SBs to increase the digital and analog I/O capability.

You can add a BB to provide long-term backup of the CPU's real-time clock.

NOTE

BBs do not have a removable communication port or I/O wiring connector feature like CBs and SBs.

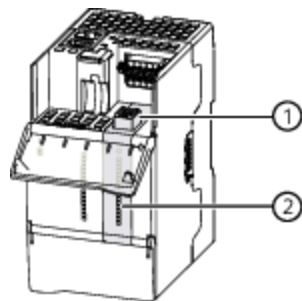
All S7-1200 G2 CPUs support plug-in expansion boards:

- The 1212 CPUs support one plug-in expansion board.
- The 1214 CPUs support two plug-in expansion boards.

NOTE

You can use any combination of plug-in expansion boards in a 1214C or 1214FC CPU, but you cannot use two BBs at the same time. Only one BB can be used. You cannot configure more than one BB for any S7-1200 G2 CPU the TIA Portal. All S7-1200 G2 CPUs support one BB.

In the following diagram, the plug-in expansion board is highlighted, and its key features are labeled:

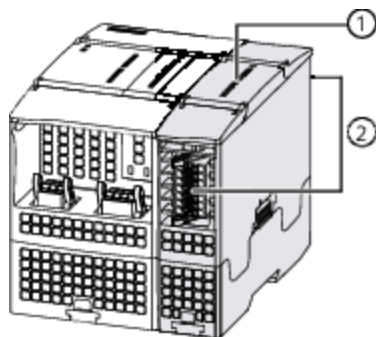


- ① Removable communication port or I/O wiring connector (This feature is not present on BBs.)
- ② Status LEDs

Communication modules (CMs) and Communication processors (CPs)

CMs and CPs add communication options to the system, such as RS232/422/485 and Ethernet connectivity. You connect CMs and CPs to the right side of a CPU or CM. All S7-1200 G2 CPUs support up to three communication devices, CMs and CPs, in any combination.

In the following diagram, a CM or CP is highlighted, and its key features are labeled:



- ① Status LEDs
- ② Removable communication connector

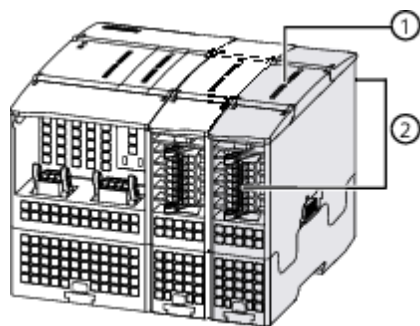
Signal modules (SMs)

SMs add additional functionality to the system, such as digital and analog I/O capability. Connect SMs to the right side of a CPU, CM, CP, or SM. The number of supported expansion modules depends on the CPU:

- The 1212 CPUs support up to six expansion modules (CMs, CPs, and SMs).
- The 1214 CPUs support up to ten expansion modules (CMs, CPs, and SMs).

To determine the number of SMs you can use in a system, subtract the number of CMs or CPs from the maximum number of expansion modules supported. For example, if you use three CMs or CPs with a 1212 CPU, you can use three SMs.

In the following diagram, the SM is highlighted, and its key features are labeled:



- ① Status LEDs
- ② Removable I/O wiring connector

3.3 Features

The S7-1200 G2 PLC (Page 57) provides the following features:

- Savings in Installation and wiring (Page 63) space
- Faster execution times
- Near Field Communication (NFC) (Page 315) application for mobile device access to the CPU
- Two expansion board slots (Page 59) for 1214 CPU models, one slot for 1212 CPU models
- Dual Ethernet ports for all CPU models
- Enhanced security
- 8 HSCs (High Speed Counters)
- 8 pulse generators for use as PTOs (Pulse Train Outputs) or for PWM (Pulse Width Modulation)
- Additional error OBs (Page 106)
- Basic, standard, and advanced motion control features (Page 318)
- Support for Real-Time PROFINET and Isochronous Real-Time PROFINET communication
- Ability for CPU can to act as an I-device with PROFIenergy functionality
- Support for Media Redundancy for Planned Duplication (MRPD) (Page 264) and Media Redundancy Protocol (MRP) (Page 264)
- Support for 31 PROFINET devices (Page 214)
- User-configurable alarms
- Web server (Page 316)
- Support for DHCP and DNS (Page 240)
- Work memory reporting as code work memory and data work memory
- Power budget calculation tool in TIA Portal
- 8MB of internal load memory
- 20KB of retentive memory
- System logging (Page 43)
- Support for users and roles (Page 158)
- SIMATIC Controller Profiling
(<https://support.industry.siemens.com/cs/ww/en/view/109750245>)
- OPC UA server (Page 273)
- Backup and restore capability (Page 354)

Refer to the Technical Specifications (Page 356) for more information.

Differences from the S7-1200 family

The S7-1200 G2 PLC (Page 57) provides features and differences from the S7-1200 PLC as described in Comparison to S7-1200 (Page 507).

3.4 What's new?

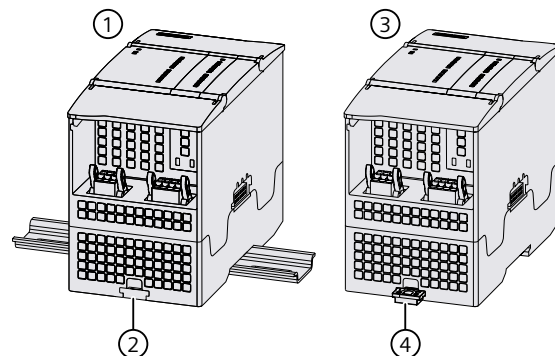
The following features are new with this release:

- OPC UA server (Page 273)
- System web pages for the Web server (Page 316)
- Additional modules:
 - Battery Board (BB) 1297 (Page 488)
 - Communication Processor (CP) 1243-1 G2 Ethernet (Page 489)
 - Input Simulators (8 position and 14 position) (Page 495)
 - Signal Module (SM) 1223 DI 16x24VDC / DQ 16xrelay (Page 430)
 - Signal Module (SM) 1223 DI 16x24VDC / DQ 16x24VDC Sink (Page 428)
 - Signal Module (SM) 1223 DI 16x24VDC / DQ 16x24VDC (Page 425)
- Additional spare parts:
 - CB PtP terminal block (Page 501)
 - CM PtP terminal block (Page 501)
- Support for central users on UMC server (Page 158)
- Backup and Restore (Page 354)
- Modbus TCP redundancy instructions (Page 311)
- PROFINET security class 1 (Page 214)
- Communication load default of 20% (Page 128)
- Support for a nesting depth of 26 hierarchical levels of Structs
- Support for Pulse Train Outputs (PTOs) in Motion control (https://docs.tia.siemens.cloud/access?ft:originId=/.84171825419/86376357131_enUS.htm)
- Additional Motion Control (Page 318) functionality
- Enhanced support for S7-1200 G2 Near Field Communication (NFC) (Page 315)

Installation and wiring

4.1 Installation guidelines

You can install an S7-1200 G2 either on a standard DIN rail or on a panel, and you can orient the S7-1200 G2 either horizontally or vertically. The small size of the S7-1200 G2 allows you to make efficient use of space.



- ① DIN rail installation
- ② DIN rail clip in latched position

- ③ Panel installation
- ④ DIN rail clip in extended position for panel mounting

The S7-1200 G2 family provides a variety of expansion modules that you can use to increase the capabilities of the CPU with additional I/O or other communication protocols. For detailed information on a specific module, see the technical specifications ([Page 356](#)).

Electrical equipment standards classify the SIMATIC S7-1200 G2 system as Open Equipment. You must install the S7-1200 G2 in a housing, cabinet, or electric control room. Only allow authorized personnel access to the housing, cabinet, or electric control room.

Provide a dry environment for installation of the S7-1200 G2. SELV/PELV circuits provide protection against electric shock in dry locations.

Provide appropriate mechanical strength, flammability protection, and stability protection for open equipment in your location according to applicable electrical and building codes.

Conductive contamination due to dust, moisture, and airborne pollution can cause operational and electrical faults in the PLC.

If you locate the PLC in an area where conductive contamination might be present, protect the PLC in an enclosure with appropriate protection rating. IP54 is one rating for electronic equipment enclosures in dirty environments and might be appropriate for your application.

 WARNING

Risks associated with improper installation

Improper installation of the S7-1200 G2 can result in electrical faults or unexpected operation of machinery.

You must follow all instructions for installation and maintenance of a proper operating environment to ensure that the equipment operates safely.

Electrical faults or unexpected machine operation can result in death, severe personal injury, and/or property damage.

Separating S7-1200 G2 devices from heat, high voltage, and electrical noise

When configuring the layout of S7-1200 G2 devices in a panel, always do the following:

- Separate the devices that generate high voltage and high electrical noise from the low-voltage, logic-type devices such as the S7-1200 G2.
- Place electronic-type devices in the cooler areas of the cabinet away from heat-generating devices to reduce exposure to high-temperatures and extend the operating life of the devices.
- Avoid placing low-voltage signal wires and communications cables in the same tray with AC power wiring and high-energy, rapidly-switched DC wiring when routing wiring for the devices.

Providing adequate clearance for cooling and wiring

The design of S7-1200 G2 devices provides for natural convection cooling. For proper cooling, allow at least 25 mm of clearance above, below, and on both sides of the system. Also, allow at least 25 mm of depth between the front of the modules and the inside of the enclosure.

 CAUTION

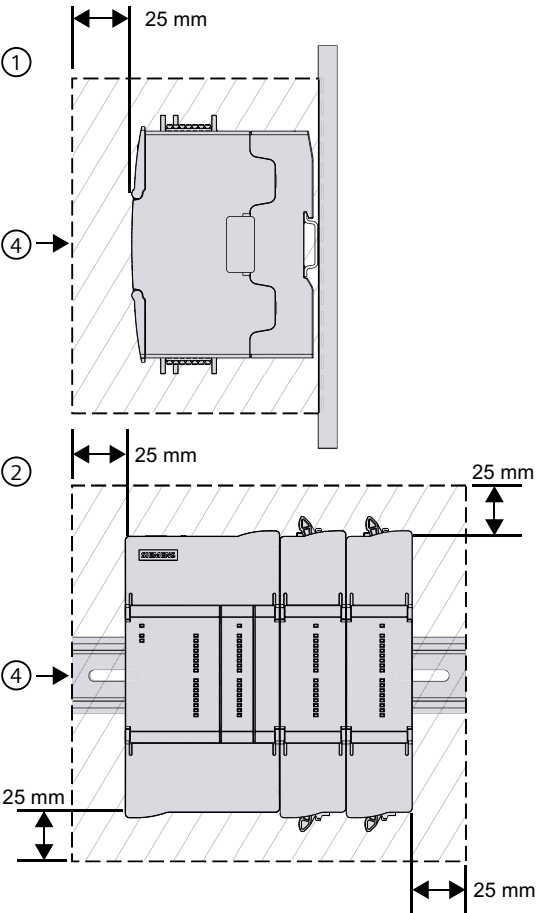
Effect of vertical mounting on allowable ambient temperature

Vertical mounting reduces the maximum allowable ambient temperature.

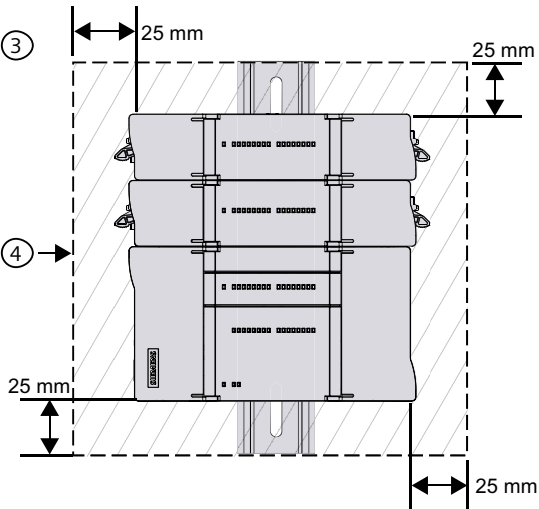
Orient a vertically mounted S7-1200 G2 system as shown in the following figure: the CPU, when vertically mounted, is at the bottom with its left side down. Ensure that the S7-1200 G2 system is mounted correctly.

Improper installation of a vertically mounted system can result in personal injury.

When planning your layout for the S7-1200 G2 system, allow enough clearance for the wiring and communications cable connections.



① Side view
② Horizontal installation



③ Vertical installation
④ Clearance area

4.2 Safety information

Before you install or remove any electrical device, ensure that the power to that equipment has been turned off. Also, ensure that the power to any related equipment has been turned off.

 **WARNING**

Risk of electrocution when installing or removing devices

Installing or wiring the S7-1200 G2 or related equipment with power applied could cause electric shock or unexpected operation of equipment.

Always follow appropriate safety precautions and ensure that power is disabled to the S7-1200 G2 or related equipment before attempting to install or remove any devices.

Failure to disable all power to the S7-1200 G2 and related equipment during installation or removal procedures could result in death, severe personal injury, and/or property damage due to electric shock or unexpected equipment operation.

Always ensure that whenever you replace or install an S7-1200 G2 device you use the correct module or equivalent device.

Always be sure to follow the guidelines for grounding [\(Page 86\)](#).

 WARNING

Risks associated with replacing S7-1200 G2 devices

Incorrect installation of an S7-1200 G2 module can cause the program in the S7-1200 G2 to function unpredictably.

Use the same model, orientation, and order when replacing an S7-1200 G2 device.

Failure to do so can cause unexpected equipment operation resulting in death, severe personal injury, and/or property damage.

 WARNING

Installing or removing devices in a flammable or combustible atmosphere

Disconnecting equipment in a flammable or combustible atmosphere can cause a fire or an explosion.

Do not disconnect equipment in a flammable or combustible atmosphere; follow appropriate safety precautions when working in a flammable or combustible atmosphere.

A fire or explosion can result in death, serious injury, and/or property damage.

NOTICE

Risks associated with electrostatic discharge

Electrostatic discharge can damage the memory card or the receptacle on the CPU. If damaged, the receptacle or memory card can malfunction or become inoperable.

To protect the memory card and receptacle from electrostatic discharge, do the following:

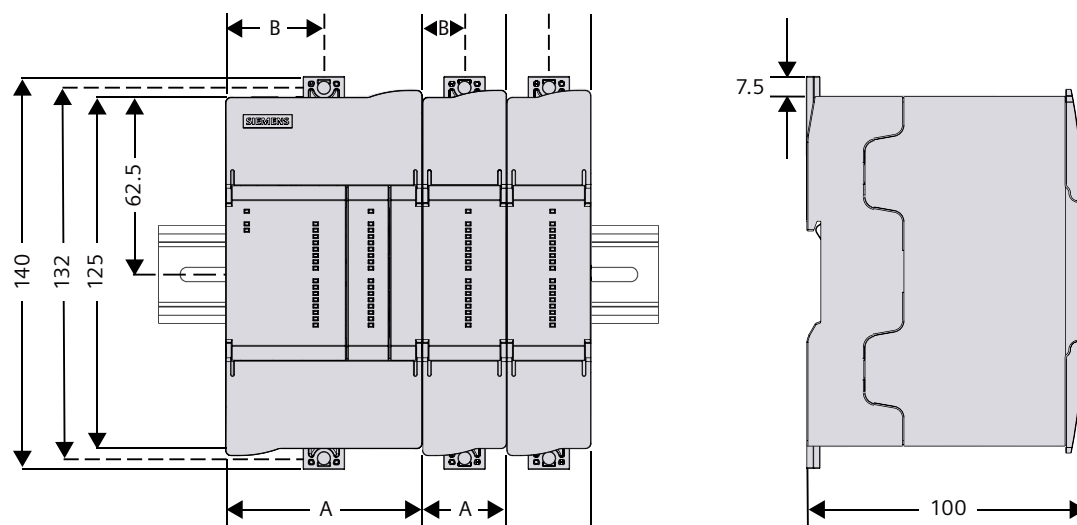
- Make contact with a grounded conductive pad or wear a grounded wrist strap when handling the memory card.
- Store the memory card in a conductive container.

Receptacle or memory card malfunction can result in property damage.

4.3 Mounting dimensions

Use the following mounting dimensions to ensure proper device installation. All mounting dimensions are shown in millimeters (mm).

CPU 1212C



CPU 1214C

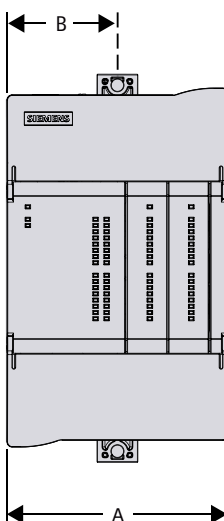


Table 4-1 Mounting dimensions (mm)

S7-1200 G2 Devices		Width A (mm)	Width B (mm)
CPUs ¹	CPU 1212C (AC/DC/Rly, DC/DC/Rly, and DC/DC/DC)	70	35
	CPU 1214C (AC/DC/Rly, DC/DC/Rly, and DC/DC/DC)	80	40
Fail-safe CPUs ¹	CPU 1212FC (DC/DC/Rly, and DC/DC/DC)	70	35

¹ If you plan to use an input simulator, you must have extra clearance. See the Input simulators section of the Technical specifications chapter for specific dimensions.

4.4 Providing power for the CPU

S7-1200 G2 Devices		Width A (mm)	Width B (mm)
Fail-safe CPUs ¹	CPU 1214FC (DC/DC/Rly, and DC/DC/DC)	80	40
Signal modules	SM 1221 (16 DI 24V)	30	15
	SM 1222 (16 DQ 24V and 16 Rly)	30	15
	SM 1223 (8 DI / 8 DQ, 8 DI / 8 Rly)	30	15
	SM 1223 (16 DI / 16 DQ, 16 DI / 16 Rly, 16 DI / 16 DQ Sink)	50	25
	SM 1223 (8 DI / 8 DQ, 8 DI / 8 Rly, 16 Rly, 16 DI / 16 DQ Sink, and 16 DI / 16 DQ)	30	15
	SM 1231 (8 AI)	30	15
	SM1232 (8 AQ)	30	15
	SM 1233 (4 AI / 4 AQ)	30	15
	SM 1231 (8 TC and 4 RTD)	30	15
Communication modules	CM 1241 (RS485/232/422)	30	15
Communication processors	CP 1243-1 G2 Ethernet	30	15

¹ If you plan to use an input simulator, you must have extra clearance. See the Input simulators section of the Technical specifications chapter for specific dimensions.

Each CPU, SM, and CM supports mounting on either a DIN rail or on a panel. Use the DIN rail clips on the module to secure the device on the rail. These clips also snap into an extended position to provide screw mounting positions to mount the unit directly on a panel.

Always be sure to follow the guidelines for grounding [\(Page 86\)](#).

See also

[Input simulators \(Page 495\)](#)

4.4 Providing power for the CPU

All S7-1200 G2 CPUs have an internal power supply that provides power to the CPU, any expansion modules or boards, and the 24 V DC Sensor power output.

You can connect any of the following to the CPU:

- Signal boards
- Communication modules
- Signal modules

Plug-in expansion boards, such as signal boards (SBs), install into the front of the CPU.

Communication modules (CM) and signal modules (SM) are installed to the right of the CPU. You can connect a CM to the right of a CPU or another CM. You can connect an SM to the right of a CPU, CM, or another SM.

The maximum number of expansion modules allowed for each CPU can be found in the Technical specifications [\(Page 356\)](#) under the CPU's General specifications and features.

For more information on expansion modules, see S7-1200 G2 modules [\(Page 59\)](#).

All S7-1200 G2 CPUs have a power budget calculator (Page 169) in the STEP 7 project. Select the CPU in Device view and navigate to the General tab > System power supply > Power segment overview to view the Power consumption per module and the Summary for the hardware configuration. When the chosen hardware configuration exceeds the available power budget, a compile warning is given.

Some of the 24 V DC power input ports in the PLC system are interconnected with a logic common circuit connecting multiple M terminals. The CPU 24 V DC power supply input, the SM relay coil power input, and a non-isolated analog power supply input are examples of circuits that are interconnected when designated as not isolated in the data sheets. All non-isolated M terminals must connect to the same external reference potential.

 WARNING

Risks with connecting non-isolated M terminals to different reference potentials

Connecting non-isolated M terminals to different reference potentials causes unpredictable current flows. Unpredictable current flows can cause PLC damage or abnormal PLC and equipment operation.

Always ensure that all non-isolated M terminals in a PLC system are connected to the same reference potential.

PLC damage or abnormal PLC and equipment operation can cause death, severe personal injury, and/or property damage.

Each CPU supplies DC power:

- Each CPU has a 24 V DC sensor supply that can supply 24 V DC for local input points, for relay coils on the expansion modules, or for other requirements. If your 24 V DC power requirements exceed the budget of the sensor supply, you can add an external 24 V DC power supply to your system. You must manually connect the external 24 V DC supply to the input points or relay coils on the expansion modules.

 WARNING

Risks with parallel connections

Connecting an external 24 V DC power supply in parallel with the CPU's DC sensor supply can result in a conflict between the two supplies as each seeks to establish its own preferred output voltage level.

When using the CPU's DC sensor supply in conjunction with an additional external 24 V DC power supply, they must not be wired in parallel.

Doing so could cause unpredictable operation of the PLC system, resulting in death, severe personal injury, and/or property damage.

Maximum applied voltage to S7-1200 G2 Fail-safe devices

When providing power for the S7-1200 G2 Fail-safe CPUs, you must observe the following:

- **Operational voltage:** The operational voltage of the fail-safe CPUs and fail-safe SMs is 20.4 V DC - 28.8 V DC. Design and testing assure operation of the unit to specifications. Defined transients from defined source impedances per EN 61000-4-2, 61000-4-4, and 61000-4-6, as specified in the data sheet for each product, can be imposed on this voltage without disrupting operation or causing damage. Sustained operation in the range of 28.8 - 35 V DC can result in unacceptable temperature rise and thermal damage, causing the product to become inoperable.
- **Absolute maximum rating regarding supply voltage:** The absolute maximum rating to prevent module damage and to ensure the functional safety of the modules is 35 V DC. The manufacturer must specify these power supplies to limit the output voltage to 35 V DC or less under fault conditions. Otherwise, you must supply external protection that reliably opens the circuit or limits the output voltage to less than 35 V DC to the fail-safe CPU and fail-safe SMs.
- **Immunity to surge voltages (Page 356):** To meet the product standard for burner controls (EN 298), the wiring must be equipped with external protection against coupled surge voltages caused by lightning. For more information, refer to the function manual "*Designing interference-free controllers*" (<https://support.industry.siemens.com/cs/ww/en/view/59193566>).

Requirements for power supplies in the event of voltage interruption

To ensure adherence to IEC 61131-2, only use power packs/power supply units with a main buffering time of at least 10 ms for DC power or 1/2 AC cycle. The port that powers the CPU meets IEC61131-2 rating of PS2 with an interruption time of 10 ms for DC power and 1/2 AC cycle for AC power. Observe the relevant requirement in your product standards (for example, 30 ms for Burner applications according to EN 298) regarding possible voltage interruptions. The latest information on PS components is available on the Internet (<https://support.industry.siemens.com/>).



WARNING

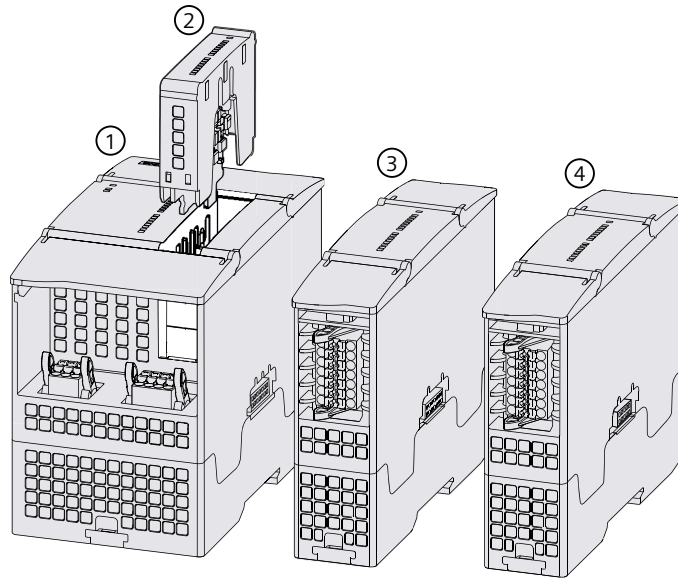
All power supply and fail-safe SM circuits must be connected together to a common voltage reference or must be isolated SELV circuits.

The power supply M terminals on the fail-safe CPU and the fail-safe SMs must be connected together or isolated as SELV. Failure to do so can result in unexpected machine or process operation.

Connecting all M terminals together or isolating with approved SELV isolation prevents unwanted current flows in the event of a single fault in the CPU to SM isolation boundary.

Unexpected machine or process operation can result in death or serious injury to personnel, and/or damage to equipment.

4.5 Expansion capability of the CPU



- ① Central processing unit (CPU)
- ② Expansion board
- ③ Communication module (CM), if used
- ④ Signal module (SM)

4.6 Installation and removal procedures

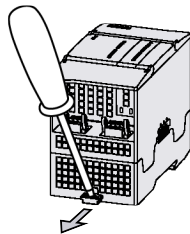
4.6.1 Installing and removing a CPU

You can install the S7-1200 G2 CPU on a DIN rail or a panel.

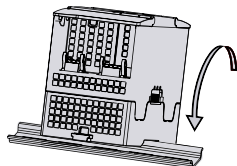
Installing the CPU on a DIN rail

To install the CPU on a DIN rail, follow these steps:

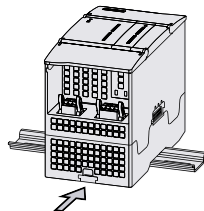
1. Install the DIN rail; secure the rail to the mounting panel every 75 mm.
2. Ensure that the CPU and all S7-1200 G2 equipment are powered down.
3. Use an M3 screwdriver to extend the lower DIN rail clip on the CPU to allow it to fit over the rail.



4. Hook the CPU over the top of the DIN rail.
5. Rotate the CPU down into position on the rail.



6. Push in the lower DIN rail clip to secure it to the rail.



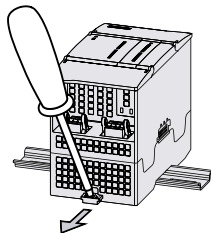
NOTE

Using DIN rail stops can be helpful if the CPU is in an environment with high vibration potential or if the CPU has been installed vertically. Use an end bracket (8WA1808 or 8WA1805) on the DIN rail to ensure that the modules remain connected.

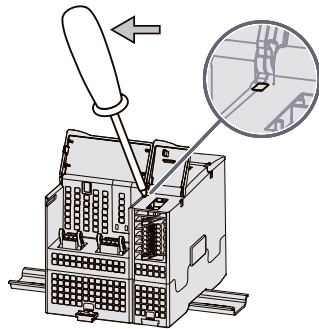
Removing the CPU from a DIN rail

To remove the CPU from a DIN rail, follow these steps:

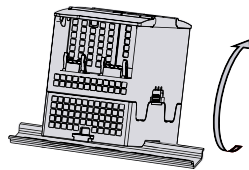
1. Ensure that the CPU and all S7-1200 G2 equipment are powered down.
2. Disconnect the I/O connectors, wiring ([Page 79](#)), and cables from the CPU.
3. Use an M3 screwdriver to extend the lower DIN rail clip on the CPU to release it from the rail.



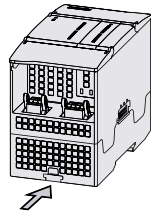
4. If the CPU is connected to an SM or CM, place an M3 screwdriver between the CPU and connected module; gently pry left to disconnect the CPU.



5. Rotate the CPU up and off the rail and remove the CPU from the system.



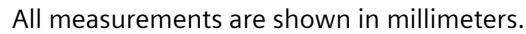
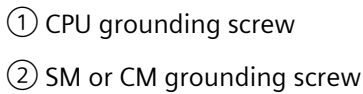
6. Push in the DIN rail clip to protect it from damage.



Installing the CPU on a panel

To install the CPU on a panel, follow these steps:

1. Locate, drill, and tap the mounting holes (M4), using the dimensions shown in the diagrams below.
2. Using the Guidelines for grounding ([Page 86](#)), install an M4 pan head stainless steel screw with a star washer into the panel at the grounding screw locations shown below.
3. Ensure that the CPU and all S7-1200 G2 equipment are powered down.
4. Use a screwdriver to extend the upper and lower DIN rail clips on the CPU.
5. Secure the module to the panel, using a Pan Head M4 screw with spring and flat washer; apply the appropriate torque to compress the spring washer.



Installing and removing a CM or SM

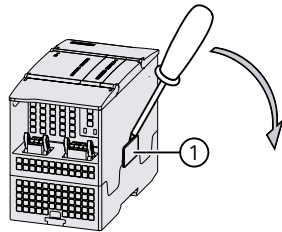
Before you install or remove any electrical device, ensure that the power to that equipment has been turned off. Also, ensure that the power to any related equipment has been turned off.

Failure to disable all power to the S7-1200 G2 and related equipment during installation or removal procedures can result in death, severe personal injury and/or property damage due to electric shock or unexpected equipment operation.

Installing a CM or SM

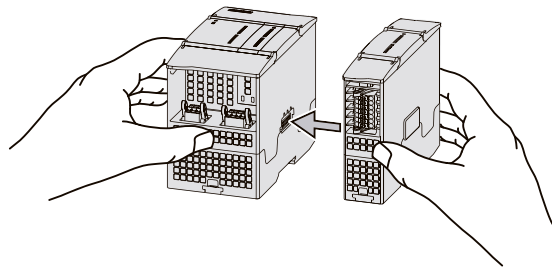
To install an CM or SM, follow these steps:

1. Ensure that the CPU and all S7-1200 G2 equipment are powered down.
2. Remove the bus cover from the right side of the CPU or module. Insert a screwdriver into the slot above the bus cover, gently pry the cover loose, and remove it. Retain the cover for reuse.



① Bus cover

3. If you are installing the module on a DIN rail extend the lower DIN rail clip, hook the module over the top of the rail, and rotate the module down into place.
4. Align the bus connector and the posts of the module with the holes of the CPU or module, and firmly press the units together until the posts snap into place.



5. If you are DIN Rail mounting, push the lower DIN rail clip in to secure the module. If you are panel mounting, screw the module to the panel.

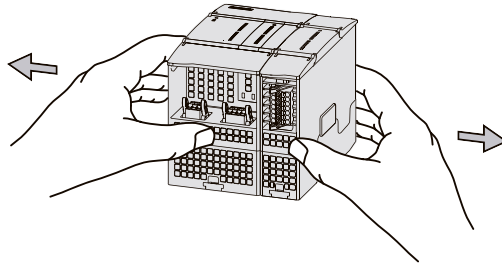
Removing a CM or SM

To remove an CM or SM, follow these steps:

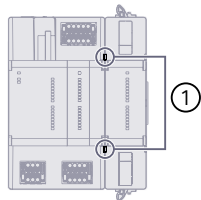
1. Ensure that the CPU and all S7-1200 G2 equipment are powered down.
2. Remove the I/O connectors and all wiring and cables from the module.
3. If the module is mounted on a DIN rail, use an M3 screwdriver to extend the lower DIN rail clip on the module. If the module is panel mounted, remove the mounting screws from the upper and lower DIN rail clips to release it from the panel.

Note: In some cases, it may be necessary to loosen other devices mounted to the left or right to create room to disconnect the device you wish to remove.

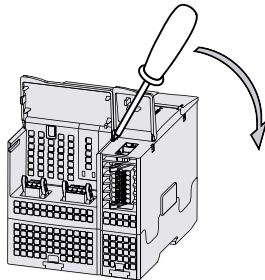
4. Separate the module from the CPU or module using one of the following methods:
 - Grasp the units and pull them apart.



- Place an M3 screwdriver in the provided slot under the doors and pry the devices apart.



① Slots for screwdriver



5. Remove the module(s) from the DIN rail or panel; if removing a module(s) from a DIN rail, rotate it up and off the rail.
6. Push in the DIN rail clips on the modules you are removing to protect them from damage.

4.6.3 Installing and removing expansion boards

Installing or removing an SB

You can install one plug-in expansion board to CPU 1212 and two plug-in expansion boards of any type to CPU 1214.

Before you install or remove any electrical device, ensure that the power to that equipment has been turned off. Also, ensure that the power to any related equipment has been turned off.

WARNING

Installation or removal of S7-1200 G2 devices with power applied

Installation or removal of S7-1200 G2 or related equipment with the power applied can cause electric shock or unexpected operation of equipment.

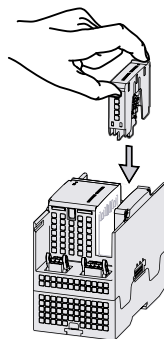
Always follow appropriate safety precautions and ensure that power to the S7-1200 G2 is disabled before attempting to install or remove S7-1200 G2 CPUs or related equipment.

Failure to disable all power to the S7-1200 G2 and related equipment during installation or removal procedures can result in death, severe personal injury and/or property damage due to electric shock or unexpected equipment operation.

Installing an SB

To install an SB, follow these steps:

1. Ensure that the CPU and all S7-1200 G2 equipment are powered down.
2. Remove the upper and lower doors from the CPU.
3. Grasp the top and bottom of the existing blank board cover or plug-in expansion board, and pull away from the CPU to remove it. (If you are installing an SB into a newly purchased CPU, retain the preinstalled blank board cover after removing it from the CPU.)

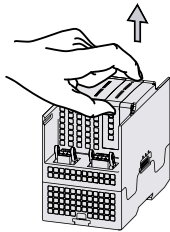


4. Insert the plug-in expansion board into the vacant slot and press down on it until it clicks into place.
5. Replace the upper and lower doors.

Removing an SB

To remove an SB, follow these steps:

1. Ensure that the CPU and all S7-1200 G2 equipment are powered down.
2. Remove the upper and lower doors from the CPU.
3. Grasp the top and bottom of the plug-in expansion board and pull away from the CPU to remove it.



4. Insert the desired plug-in expansion board into the vacant slot and press down on it until it clicks into place. (If no SB is required, reinsert the blank board cover that came with the CPU.)
5. Replace the upper and lower doors.

WARNING

Risks associated with leaving a plug-in expansion board slot empty

Leaving a plug-in expansion board slot empty can expose the internal elements of the CPU to environmental contaminants like moisture, dust, or debris that can damage or shorten the lifespan of the CPU.

Do not leave a plug-in expansion board slot empty. If you are not installing a new SB, reinsert the blank board cover. (Blank board covers are preinstalled in the CPU at the time of purchase.)

Damage to the CPU can cause equipment malfunction. Equipment malfunction can potentially result in property damage, severe personal injury, or death.

4.6.4 Removing and installing terminal block connectors

Removing and installing a CPU, CM, or SM terminal block connector

All S7-1200 G2 devices provide removable connectors to make connecting the wiring easy. For more information on how to wire connectors, see Wiring procedures [\(Page 88\)](#).

Installation risks with terminal block connectors in relay signal modules

You can incorrectly install a CPU's high voltage 6, 8, or 12 pin terminal block connector into a relay digital signal module and a CPU's high voltage 6 or 8 pin terminal block connector into an relay analog signal module.

The existing keying on the CPU's high voltage terminal block connectors does not prevent you from installing them into the following relay signal modules:

Signal modules (SMs)	Article number
SM 1222 DQ 16xRelay (Page 418)	6ES7222-5HH50-0XB0
SM 1223 DI 8x24VDC / DQ 8xRelay (Page 423)	6ES7223-5PH50-0XB0
SM 1231 AI 8x14bit (Page 433)	6ES7231-4HF50-0XB0
SM 1232 AQ 8x14bit (Page 436)	6ES7232-4HF50-0XB0
SM 1233 AI 4x14bit / AQ 4x14bit (Page 438)	6ES7233-4HF50-0XB0

WARNING

Risk of electrocution with improper terminal block installation

If you install a 6, 8, or 12 pin high voltage connector from a relay CPU into one of the relay SMs listed above, hazardous levels of voltage can occur on the DIN rail and connected machinery.

Ensure that the terminal block connector and the connector receptacle on the device have the same number of pins before installing the terminal block connector, and that both levers of the connector are in the locked position before restoring power to the system.

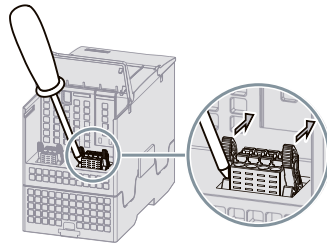
Death, severe personal injury, and property damage can result if you install a relay CPU's 6, 8, or 12 pin high voltage connector into one of the relay SMs listed above.

Removing a CPU, CM, or SM terminal block connector

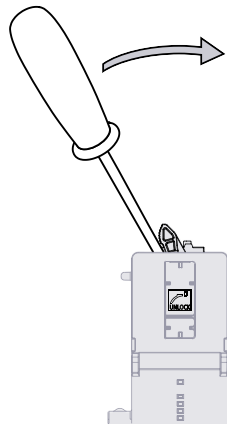
To remove an CPU, CM, or SM terminal block connector, follow these steps:

1. Ensure that the CPU and all S7-1200 G2 equipment are powered down.
2. Use a screwdriver to release the terminal block connector levers or firmly press them in the direction shown below.

CPU removal:



CM or SM removal:



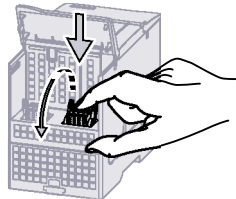
3. Grasp the connector and remove it from the CPU, CM, or SM.

Installing a CPU, CM, or SM terminal block connector

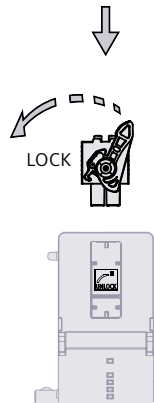
To install an CPU, CM, or SM terminal block connector, follow these steps:

1. Ensure that the CPU and all S7-1200 G2 equipment are powered down.
2. Align the terminal block connector with the pins on the unit; for the SM and CM you can use the symbol marked on the unit to identify proper orientation of the connector.
3. Press firmly down on the center of the terminal block connector until it snaps into place. (The levers will rotate and lock into place as you press down.)

CPU installation:



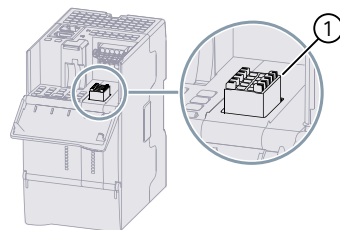
CM or SM installation:



4. Make sure that the terminal block connector is properly aligned and in the locked position.

Removing and installing an SB terminal block connector

The terminal block connector for an SB is behind the top door of the CPU, as shown below.

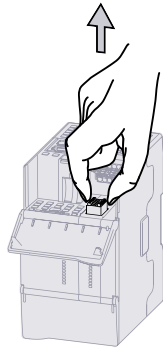


① SB terminal block connector

Removing an SB terminal block connector

To remove an SB terminal block connector, follow these steps:

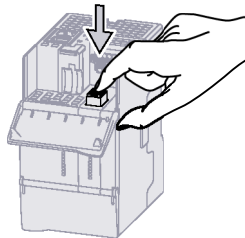
1. Ensure that the CPU and all S7-1200 G2 equipment are powered down.
2. Firmly grasp the terminal block connector and pull away from the CPU.



Installing an SB terminal block connector

To install an SB terminal block connector, follow these steps:

1. Ensure that the CPU and all S7-1200 G2 equipment are powered down.
2. Align the terminal block connector with the pins on the unit.
3. Press down firmly on the center of the terminal block connector until it snaps into place.



4.7 Wiring guidelines and procedures

4.7.1 Safety considerations

Proper grounding and wiring of all electrical equipment are important to help ensure the optimum operation of your system and to provide additional electrical noise protection for your application and the S7-1200 G2. Refer to the technical specifications [\(Page 356\)](#) for the S7-1200 G2 wiring diagrams.

Prerequisites

Before grounding or installing wiring to any electrical device, ensure that the power to that device is off. Also, ensure that the power to any related equipment is off.

WARNING

Risk of electrocution when installing or removing devices

Installing or wiring the S7-1200 G2 or related equipment with power applied could cause electric shock or unexpected operation of equipment.

Always follow appropriate safety precautions and ensure that power is disabled to the S7-1200 G2 or related equipment before attempting to install or remove any devices.

Failure to disable all power to the S7-1200 G2 and related equipment during installation or removal procedures could result in death, severe personal injury, and/or property damage due to electric shock or unexpected equipment operation.

Always consider safety when designing the grounding and wiring for the S7-1200 G2 system. Follow all applicable electrical codes when wiring the S7-1200 G2 and related equipment. Install and operate all equipment according to all applicable national and local standards. Contact your local authorities to determine which codes and standards apply to your specific case.

WARNING

Risk of unexpected equipment operation

Control devices can fail in unsafe conditions, resulting in unexpected equipment operation.

Use an emergency stop function, electromechanical overrides, or other redundant safeguards that are independent of the S7-1200 G2.

Unexpected operation can result in death, severe personal injury and/or property damage.

4.7.2 Guidelines for isolation

S7-1200 G2 AC power supply boundaries and I/O boundaries to AC circuits provide safe separation between AC line voltages and low voltage circuits. These boundaries include double or reinforced insulation, or basic plus supplementary insulation, according to various standards. Components which cross these boundaries such as optical couplers, capacitors, transformers, and relays have been approved as providing safe separation. Only circuits rated for AC line voltage include safety isolation to other circuits. Isolation boundaries between 24 V DC circuits are functional only. Do not depend on these boundaries for safety.

The sensor supply output, communications circuits, and internal logic circuits of an S7-1200 G2 with included AC power supply are sourced as SELV (safety extra-low voltage) according to EN 61131-2.

To ensure safe operation, you must power the external connections to the following items from approved sources that meet the requirements of SELV/PELV, Class 2, Limited Voltage, or Limited Power according to various standards:

- Communications ports

The CPU meets isolation requirements between the ports and internal circuits (1500 V AC) according to IEEE 802.3, Chapter 27.5.3, Environment B. Therefore, do not connect LAN or LAN segments of different environments (for example, Environment A and B according to IEEE 802.3) to the dual ports of S7-1200 G2 CPUs.

- Analog circuits
- 24 V DC nominal power supply
- Digital I/O circuits

WARNING

Risk of electrocution with use of non-isolated or single insulation supplies

Using non-isolated or single insulation supplies can cause circuits that are normally safe to the touch, like communications circuits and low voltage sensor wiring, to carry hazardous levels of voltage.

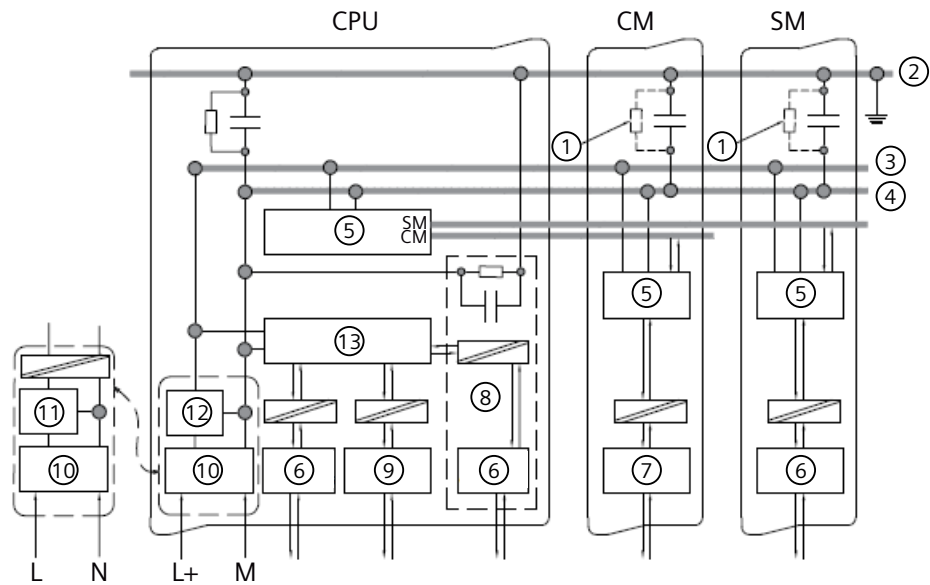
Do not use non-isolated or single insulation supplies to supply low voltage circuits from an AC line.

Only use high voltage to low voltage power converters that are approved as sources of touch safe, limited voltage circuits.

Using non-isolated or single insulation supplies can cause unexpected electric shock resulting in death, severe personal injury, and/or property damage.

The following figure shows a simplified representation of the relationships of the S7-1200 G2 automation system. The electrical tie between Functional Earth and M on a G2 CPU is also represented in the figure.

The Functional Earth and Power supply common in all G2 CPUs are coupled with a series resistor and paralleled capacitor.



- ① Resistor (not present on all models)
- ② Din rail or panel
- ③ Bus 5V power
- ④ Bus common
- ⑤ Bus connection
- ⑥ Process electronics
- ⑦ Serial communication interface
- ⑧ Signal board
- ⑨ PN communication interfaces (always 2 per CPU)
- ⑩ Filter
- ⑪ AC power
- ⑫ DC power
- ⑬ Electronics

4.7.3 Guidelines for grounding

Ground all S7-1200 G2 and related equipment connections (common and ground) to a single point. Always connect this single point directly to the earth ground of the system.

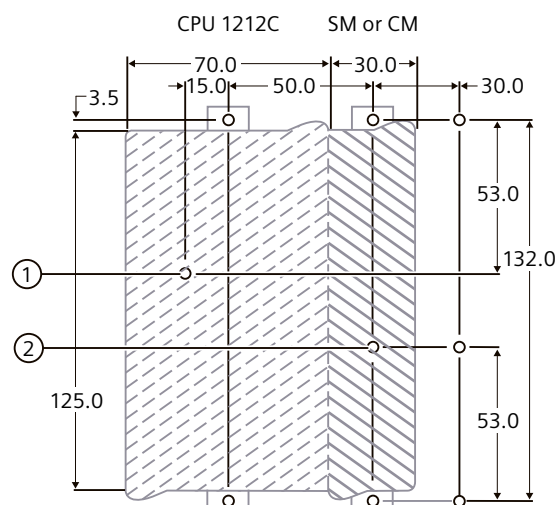
Use the shortest ground wire possible; use a large wire size, such as 2.5 mm² (14 AWG).

When using shielded cables, always connect the cable shields to the ground at both ends to reduce low and high frequency interference.

When locating grounds, consider safety-grounding requirements and the proper operation of protective interrupting devices.

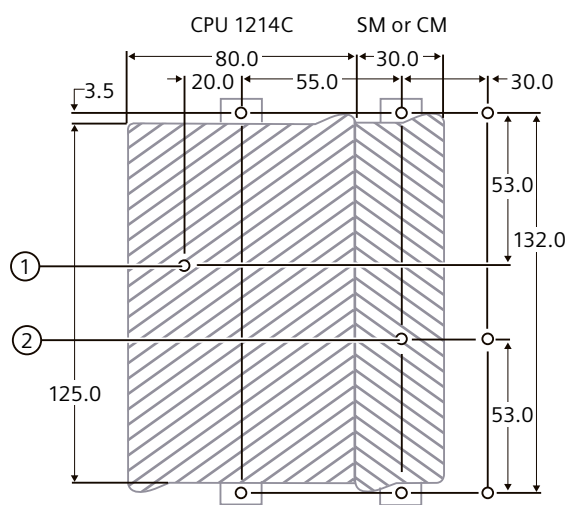
When the S7-1200 G2 is mounted to a DIN rail, the units use a spring to make proper ground connection to the DIN rail. Ensure that the DIN rail is properly grounded to the system's single point ground.

When the S7-1200 G2 is mounted to a panel, it is required to place an M4 pan head stainless steel screw with a star washer into the panel at the locations shown below. This screw will allow the units ground spring to make proper electrical contact with the panel. Ensure that the panel is properly grounded to the system's single point ground.



① CPU grounding screw

② SM or CM grounding screw



All measurements are shown in millimeters.

4.7.4 Guidelines for wiring

When designing the wiring for the S7-1200 G2, provide a single disconnect switch that simultaneously removes power from the S7-1200 G2 CPU power supply, from all input circuits, and from all output circuits. Provide over-current protection, such as a fuse or circuit breaker, to limit fault currents on supply wiring. Consider providing additional protection by placing a fuse or other current limit in each output circuit.

Install appropriate surge suppression devices for any wiring that could be subject to lightning surges.

Avoid placing low-voltage signal wires and communications cables in the same wire tray with AC wires and high-energy, rapidly switched DC wires. Always route wires in pairs, with the neutral or common wire paired with the hot or signal-carrying wire.

Use the shortest wire possible and ensure that the wire is sized properly to carry the required current. Use properly sized copper ferrule sleeves to terminate the wire into the connector.

Use wire and cable with a temperature rating that is 45 °C higher than the ambient temperature around the S7-1200 G2. Use the specific electrical circuit ratings and the installation environment to determine what other types of wiring and materials are needed.

To reduce electrical noise, use shielded wires.

In addition to using shielded wires, you can do the following to further reduce electrical noise:

- Connect the shield to the ground at both ends of the cable.
- Ground other cable shields using clamps or copper tape around the shield to provide a high surface area connection to the grounding point.

When wiring input circuits that are powered by an external power supply, include an overcurrent protection device in that circuit. External protection is not necessary for circuits that are powered by the 24 V DC sensor supply from the S7-1200 G2 because the sensor supply is already current-limited.

All S7-1200 G2 modules have removable connectors for user wiring. To prevent loose connections, ensure that the connector is seated properly, locked in place, and that the wire is installed securely into the connector.

To help prevent unwanted current flows in your installation, the S7-1200 G2 provides isolation boundaries at certain points. When planning the wiring for the system, consider these isolation boundaries. Refer to the technical specifications [\(Page 356\)](#) for the amount of isolation provided and the location of the isolation boundaries. Circuits rated for AC line voltage include safety isolation to other circuits. Isolation boundaries between 24 V DC circuits are functional only; do not depend on these boundaries for safety.

4.7 Wiring guidelines and procedures

A summary of Wiring rules for the S7-1200 G2 CPUs, CMs, SMs, SBs, and CBs is shown below:

Table 4-2 Wiring rules for S7-1200 G2 CPUs, CMs, SMs, SBs, and CBs

Wiring rules for...	CPU, CM, and SM connector	SB and CB connector ¹
Connection technology	Push in	Push in
Connectible conductor cross-sections for standard wires	0.2 mm ² to 1.5 mm ² (24 AWG to 16 AWG)	0.2 mm ² to 0.8 mm ² (24 AWG to 18 AWG)
Number of wires per connection	1 wire or combination of 2 wires in a double copper ferrule sleeve up to 1.5 mm ² (total)	1 wire or combination of 2 wires up to 0.8 mm ² (total)
Wire stripping length (Use copper ferrule sleeves for secure electric connection)	9 to 10 mm	7 mm

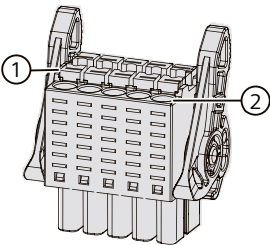
¹ Recommended ferrule sizes for SBs and CBs are listed in the Technical specifications for each board.

NOTE

Use copper ferrule sleeves on stranded conductors to reduce the risk of stray strands causing short circuits. Ferrules longer than the recommended strip length must include an insulating collar to prevent shorts due to side movement of conductors. Cross-sectional area limits for bare conductors also apply to ferrules.

4.7.5 Wiring and unwiring terminal block connectors

Removable terminal block connectors are used to wire S7-1200 G2 CPUs and modules. All S7-1200 G2 removable terminal block connectors have the following parts:



- ① Spring release
- ② Push-in terminal

There are various types and sizes of terminal block connectors. For CPU, CM, and SM terminal block connectors, the color of the terminal block lock handle and spring release indicates the type of connector. For example, an orange handle and release indicates a high voltage connector. The color used on the connector matches the color of the terminal block header on the CPU or module.

The CPU, CM, and SM terminal block connectors also have openings where you can insert a 1 mm multimeter test probe to check the voltage.

For details on the terminal block connectors used in a specific CPU or module, refer to the wiring diagram of the device in the Technical specifications (Page 356). Information on terminal block spare kits can be found in Ordering information (Page 501).

NOTE

PLCs require correct wiring to ensure safety and proper operation.

When replacing the terminal block in your S7-1200 G2 CPU or module, it is important that you use the correct terminal block and correct wiring source for your module.

The G2 removable terminal block is designed to prevent you from accidentally placing a high voltage wired terminal block into a low voltage module, or from placing a special voltage wired terminal block into a normal voltage module.

Installation risks with terminal block connectors in relay signal modules

You can incorrectly install a CPU's high voltage 6, 8, or 12 pin terminal block connector into a relay digital signal module and a CPU's high voltage 6 or 8 pin terminal block connector into an relay analog signal module.

The existing keying on the CPU's high voltage terminal block connectors does not prevent you from installing them into the following relay signal modules:

Signal modules (SMs)	Article number
SM 1222 DQ 16xRelay (Page 418)	6ES7222-5HH50-0XB0
SM 1223 DI 8x24VDC / DQ 8xRelay (Page 423)	6ES7223-5PH50-0XB0
SM 1231 AI 8x14bit (Page 433)	6ES7231-4HF50-0XB0
SM 1232 AQ 8x14bit (Page 436)	6ES7232-4HF50-0XB0
SM 1233 AI 4x14bit / AQ 4x14bit (Page 438)	6ES7233-4HF50-0XB0

WARNING

Risk of electrocution with improper terminal block installation

If you install a 6, 8, or 12 pin high voltage connector from a relay CPU into one of the relay SMs listed above, hazardous levels of voltage can occur on the DIN rail and connected machinery.

Ensure that the terminal block connector and the connector receptacle on the device have the same number of pins before installing the terminal block connector, and that both levers of the connector are in the locked position before restoring power to the system.

Death, severe personal injury, and property damage can result if you install a relay CPU's 6, 8, or 12 pin high voltage connector into one of the relay SMs listed above.

Wiring rules

For wire size requirements and wire stripping length, refer to Wiring rules for S7-1200 G2 CPUs, SMs, SBs and CBs [\(Page 87\)](#).

Solid or stranded wire can be used. With stranded wire, Siemens recommends using ferrules of an appropriate size.

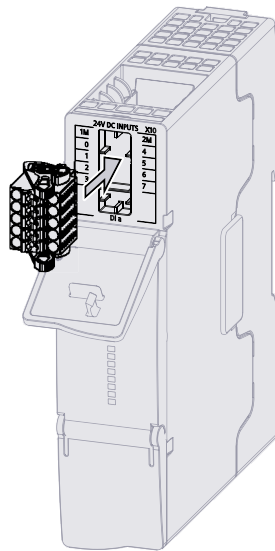
Wiring terminal block connectors

When wiring a removable terminal block connector, use a wire stripping tool to remove the plastic coating from the section of the wire that you are inserting into the connector.

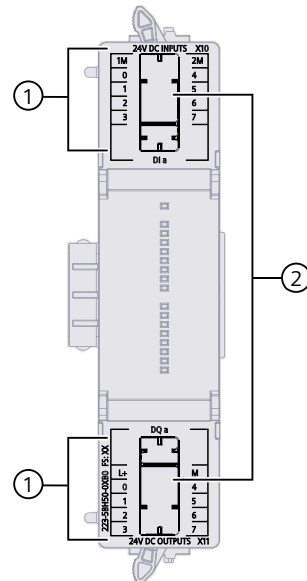
If using stranded wire, you might also need a 0.4 to 2.0 mm flat head screwdriver and a crimping tool.

To wire the removable terminal block connector of a CPU or expansion module, follow these steps:

1. Disconnect the CPU and all S7-1200 G2 equipment from electrical power.
2. Remove the terminal block connector from the CPU or module as described in Removing and installing S7-1200 G2 terminal block connectors [\(Page 79\)](#).
3. If wiring a CM or SM, place the terminal block connector into the wiring slot on the front of the module. (Skip this step if you are wiring a CPU or SB.)



Unlike the removable terminal block connectors on a CPU or SB, each expansion module has wiring slots with pin assignments located on the front of the module. Use these slots when wiring an expansion module.



- ① Pin assignments
- ② Wiring slots

4. Strip the end of the wire(s) to the length specified in Wiring rules for S7-1200 G2 CPUs, SMs, SBs and CBs [\(Page 87\)](#).

NOTE

When using stranded wire, for best results, attach a ferrule to the end of the wire and crimp the end using a crimping tool. Do not attach a ferrule to solid wire. It is not necessary to use ferrules when using solid wire.

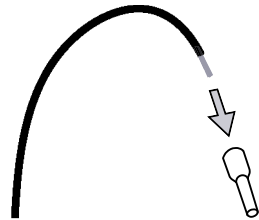
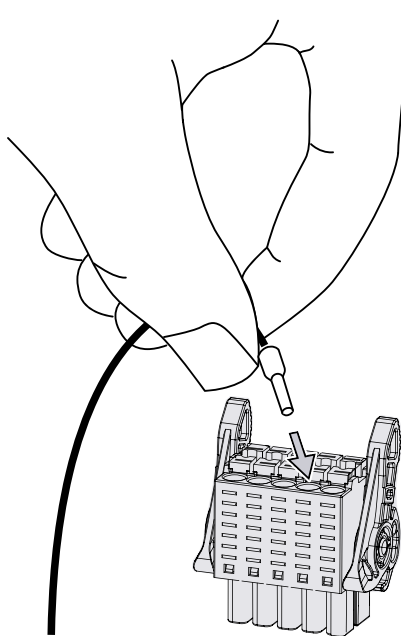
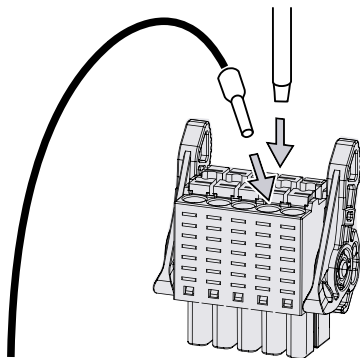


Figure 4-1 How to attach a ferrule to stranded wire

5. Use your hand to press the wire(s) into the push-in terminal,



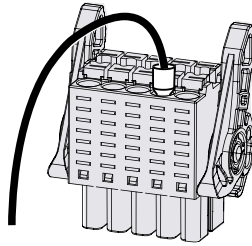
or use a 0.4 to 2.0 mm flathead screwdriver to press down on the spring release and insert the wire(s) into the push-in terminal.



NOTE

Pressing down on the spring release opens the teeth inside the connector and makes it easier to insert the wire. Once a wire is inserted into the push-in terminal, the teeth hold the wire in place.

6. Once all wires are inserted and secure, install the terminal block connector as described in Removing and installing S7-1200 G2 terminal block connectors ([Page 79](#)).

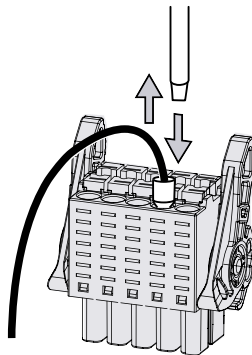


Unwiring terminal block connectors

Use a 0.4 to 2.0 mm flat head screwdriver to unwire the removable terminal block connector.

To unwire the removable terminal block connector of a CPU or expansion module, follow these steps:

1. Disconnect the CPU and all S7-1200 G2 equipment from electrical power.
2. Remove the terminal block connector from the CPU or module as described in Removing and installing S7-1200 G2 terminal block connectors ([Page 79](#)).
3. Using a 0.4 to 2.0 mm flathead screwdriver, press down on the spring release and remove the wire and ferrule from the push-in terminal.



4.7.6 Guidelines for inductive loads

Use suppressor circuits with inductive loads to limit the voltage rise when a control output turns off. Suppressor circuits protect your outputs from premature failure caused by the high voltage transient that occurs when current flow through an inductive load is interrupted.

In addition, suppressor circuits limit the electrical noise generated when switching inductive loads. High frequency noise from poorly suppressed inductive loads can disrupt the operation of the PLC. Placing an external suppressor circuit so that it is electrically across the load and physically located near the load is the most effective way to reduce electrical noise.

S7-1200 G2 DC outputs include internal suppressor circuits that are adequate for inductive loads in most applications. Internal protection is not provided for relay outputs because you can use S7-1200 G2 relay output contacts to switch either a DC or an AC load.

Consider using inductive loads with integrated suppression circuitry. However, for some applications, manufacturer-provided suppressor circuits are inadequate. You can use an additional suppressor circuit to further protect the PLC output.

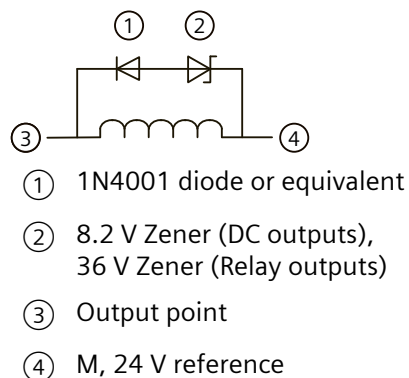
Consider using a metal oxide varistor (MOV), parallel RC circuit, or a combination of both for AC loads. A MOV suppressor with no parallel RC circuit often results in significant high frequency noise up to the clamp voltage.

A well-controlled turn-off transient will have a ring frequency of no more than 10 kHz, with less than 1 kHz preferred. Peak voltage for AC lines must be within +/- 1200 V of ground. Negative peak voltage for DC loads using the PLC internal suppression will be ~40 V below the 24 V DC supply voltage. External suppression must limit the transient to within 36 V of the supply to unload the internal suppression.

NOTE

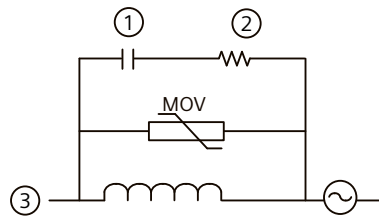
The effectiveness of a suppressor circuit depends on the application; you must verify a suppressor circuit is suitable for your particular usage. Ensure that all components are correctly rated. Use an oscilloscope to observe the turn-off transient.

Typical suppressor circuit for DC or relay outputs that switch DC inductive loads



In most applications, the addition of a diode (1) across a DC inductive load is suitable, but if your application requires faster turn-off times, then the addition of a zener diode (2) is recommended. Be sure to size your zener diode properly for the amount of current in your output circuit.

Typical suppressor circuit for relay outputs that switch AC inductive loads



① See table for C value

② See table for R value

③ Output point

Ensure that the working voltage of the metal oxide varistor (MOV) is at least 20% greater than the nominal line voltage.

Choose pulse-rated, non-inductive resistors, and capacitors recommended for pulse applications (typically metal film). Verify the components meet average power, peak power, and peak voltage requirements.

If you design your own suppressor circuit, the following table suggests resistor and capacitor values for a range of AC loads. These values are based on calculations with ideal component parameters. I rms in the table refers to the steady-state current of the load when fully ON.

Table 4-3 AC suppressor circuit resistor and capacitor values

Inductive load			Suppressor values		
I rms	230 V AC	120 V AC	Resistor		Capacitor
Amps	VA	VA	Ω	W (power rating)	nF
0.02	4.6	2.4	15000	0.1	15
0.05	11.5	6	5600	0.25	47
0.1	23	12	2700	0.5	100
0.2	46	24	1500	1	150
0.5	115	60	560	2.5	470
1	230	120	270	5	1000
2	460	240	150	10	1500

² **Conditions satisfied by the table values:**

Maximum turn-off transition step < 500 V

Resistor peak voltage < 500 V

Capacitor peak voltage < 1250 V

Suppressor current < 8% of load current (50 Hz)

Suppressor current < 11% of load current (60 Hz)

Capacitor dV/dt < 2 V/ μ s

Capacitor pulse dissipation : $\int (dv/dt) dt$ < 10000 V²/ μ s

Resonant frequency < 300 Hz

Resistor power for 2 Hz max switching frequency

Power factor of 0.3 assumed for typical inductive load

4.7.7 Guidelines for lamp loads

Lamp loads, including LED lamp loads, are damaging to relay contacts because of the high turn-on surge current. This surge current will nominally be 10 to 15 times the steady state current for a Tungsten lamp. A replaceable interposing relay or surge limiter is recommended for lamp loads that will be switched a large number of times during the lifetime of the application.

4.8 Maintenance and repair

The components of the S7-1200 G2 automation system are maintenance-free.

NOTE

Only the manufacturer can carry out repairs to the components of the S7-1200 G2 automation system.

PLC concepts, configuration, and programming

5.1 TIA Portal

The Totally Integrated Automation Portal (TIA Portal) is an engineering framework for implementing automation solutions. The TIA Portal includes STEP 7 for PLC programming and configuration. You use STEP 7 to configure CPUs and modules (Page 158) and for programming your application logic (Page 178).

TIA Portal provides an extensive information system.

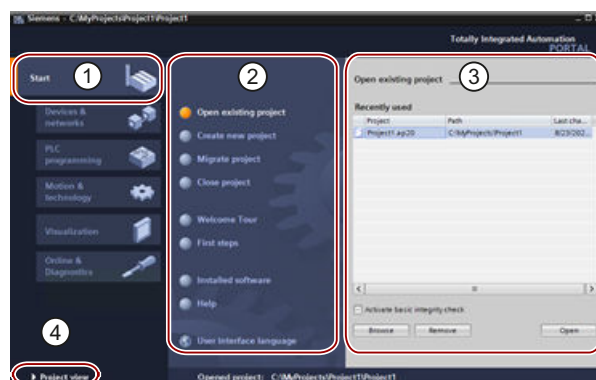
5.2 Different views in the TIA Portal

The TIA Portal provides two different views of the project that you use for your control application:

- Portal view: A task-oriented set of portals that are organized on the functionality of the tools
- Project view: A project-oriented view of the elements within the project

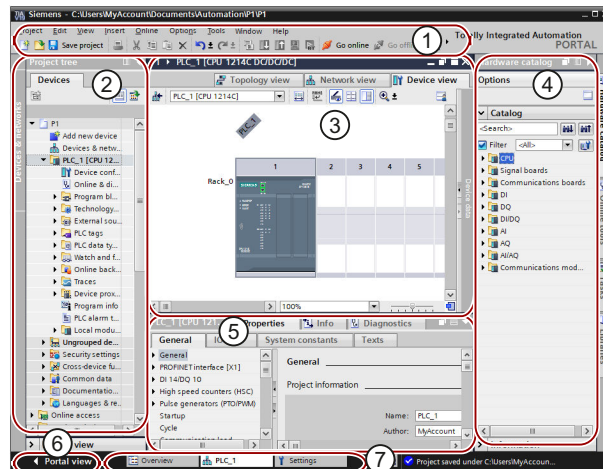
Choose which view helps you work most efficiently. With a single click, you can toggle between the Portal view and the Project view.

Portal view



- ① Portals for the different tasks
- ② Tasks for the selected portal
- ③ Selection panel for the selected action
- ④ Switch to Project view

Project view



- ① Menus and toolbar
- ② Project tree navigator
- ③ Work area
- ④ Task cards
- ⑤ Inspector window
- ⑥ Selector to change to the Portal view
- ⑦ Editor bar

With these components in one place, you have easy access to every aspect of your project. The work area consists of three tabbed views:

- Device view: Displays the device that you have added or selected and its associated modules
- Network view: Displays the CPUs and network connections in your network
- Topology view: Displays the PROFINET topology of the network including devices, passive components, ports, interconnections, and port diagnostics

Each view also enables you to perform configuration tasks. The inspector window shows the properties and information for the object that you have selected in the work area. As you select different objects, the inspector window displays the properties that you can configure. The inspector window includes tabs that allow you to see diagnostic information and other messages.

By showing all of the editors that are open, the editor bar helps you work more quickly and efficiently. To toggle between the open editors, simply click one of the open editors. You can also arrange two editors to appear together, arranged either vertically or horizontally. This feature allows you to drag and drop between editors.

5.3 Using the TIA Portal Information System

The TIA Portal Information System has extensive information about configuring and programming PLCs. In the TIA Portal Information System, refer to Help on the Information System

(https://docs.tia.siemens.cloud/access?ft:originId=../11251439499/75833983499_enUS.htm&ft:clusterId../11251439499/75833983499.htm) for usage information.

When searching for information about the S7-1200 G2, note the following:

- When filtering a search on devices, S7-1200 G2 is not available as a device selection. Filtering by S7-1500 would be the closest match to S7-1200 G2 information.
- When using context-sensitive help in the TIA Portal, if the tooltip does not include S7-1200 G2, then choose the S7-1500 topic.

This system manual for the S7-1200 G2 Programmable Logic Controller provides additional information on configuration, programming, and program execution.

5.4 Program structure

5.4.1 Structure of a STEP 7 user program

The S7-1200 G2 CPU supports the following types of code blocks that allow you to create an efficient structure for your user program:

- Organization blocks (OBs) (Page 106) define the structure of the program. Some OBs run at startup. Some run continuously when the CPU is running your process. Some run under specific conditions.
- Data blocks (DBs) (Page 136) store data that can be used by the program blocks. Refer to "Data types" (https://docs.tia.siemens.cloud/access?ft:originId=../65883487371/65883487371_enUS.htm&ft:clusterId../65883487371/65883487371.htm) in the TIA Portal Information System for descriptions of the data types that STEP 7 provides.
- Functions (FCs) and function blocks (FBs) contain the program code that corresponds to specific tasks. FCs and FBs can be called from an OB or from another FC or FB. Each FC or FB provides a set of input and output parameters for sharing data with the calling block. An FB also uses an associated data block (called an instance DB) to maintain the data values for that instance of the FB call. You can call an FB multiple times, each time with a unique instance DB. Calls to the same FB with different instance DBs do not affect the data values in any of the other instance DBs.

An S7-1200 G2 F-CPU supports the following types of code blocks that allow you to create an efficient structure for your safety program:

- F-I/O data blocks are automatically generated by the safety program when you configure an F-I/O.
- Fail-safe organization blocks (F-OBs) define the structure of the safety program. The F-OB calls the main safety block in an F-Runtime Group (F-RTG); this group contains F-blocks that you create or that are inserted from the project or global libraries, as well as those which are added automatically by the safety program. You can manage F-RTGs in the Safety Administration Editor (SAE). There can be either one or two F-RTGs.

- Fail-safe data blocks (F-DBs) store data that can be used by the safety program blocks.
 - F-shared data blocks are data blocks that contain all data shared between the safety program and the F-subsystems.
 - F-runtime group information data blocks are created by the safety program when you create an F-runtime group. These blocks provide information on the F-runtime group and on the safety program.
- Fail-safe functions (F-FCs) and Fail-safe function blocks (F-FBs) contain the program code that corresponds specifically to safety tasks. F-FCs and F-FBs can be called from an F-OB or from another F-FC or F-FB. Each F-FC or F-FB contains instructions from either the project or global library and can call other created F-FBs or F-FCs to structure the user safety program.

NOTE

Onboard standard I/O channels not used for fail-safe I/O function

In your STEP 7 project, you can configure the onboard I/O of the F-CPU with standard code blocks, but these I/O are not safety I/O. You can only use F-I/O to accomplish safety tasks by configuring the fail-safe I/O channels with safety blocks.

To learn more about the code blocks which structure the safety program, refer to the "SIMATIC Safety - Configuring and Programming" manual

(<https://support.industry.siemens.com/cs/us/en/view/54110126>).

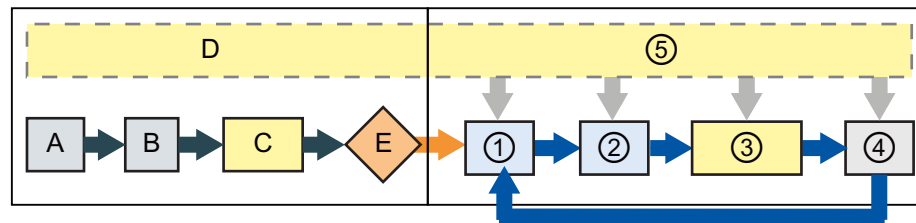
5.4.2 Execution of the user program

Execution of the user program begins with one or more optional startup OBs (Page 107) that execute once upon entering RUN mode. Execution then continues with configured program cycle OBs (Page 106) that execute cyclically. You can also associate an OB with an interrupt event, which can be either a standard event or an error event. These OBs execute whenever the corresponding standard or error event occurs.

Operating modes

The CPU has three modes of operation: STOP mode, STARTUP mode, and RUN mode. Status LEDs on the front of the CPU indicate the current mode of operation.

- In STOP mode, the CPU handles any communication requests (as appropriate) and performs self-diagnostics. The CPU does not execute the user program. Automatic updates of the process image do not occur. You can download a project to the CPU.
- In STARTUP and RUN modes, the CPU performs the tasks shown in the following figure:



STARTUP

- A Copies the state of the physical inputs to I memory
- B Initializes the Q output (image) memory area with either zero or the last value. Zeroes PN outputs
- C Initializes non-retentive M memory and data blocks to their initial value and enables configured cyclic interrupt and time of day events. Executes the startup OBs.
- D Stores any interrupt events into the queue to be processed after entering RUN mode
- E Enables the writing of Q memory to the physical outputs

RUN

- ① Writes Q memory to the physical outputs
- ② Copies the state of the physical inputs to I memory
- ③ Executes the program cycle OBs and updates the output values in the process image output area
- ④ Performs self-test diagnostics
- ⑤ Processes interrupts and communications during any part of the scan cycle

You can download some parts of a project in RUN mode (Page 340).

Restart of fail-safe system

The operating modes of the SIMATIC Safety system differ from those of the standard system only in terms of the restart characteristics.

When you switch a fail-safe CPU from STOP to RUN mode, the standard user program restarts in the usual way. When you restart the safety program, the fail-safe system initializes all data blocks with the F-Attribute with values from load memory. This is comparable to a cold restart.

Process image update and process image partitions

The CPU updates local digital and analog I/O points synchronously with the scan cycle using an internal memory area called the process image. The process image contains a snapshot of the physical inputs and outputs (the physical I/O points on the CPU, signal board, and signal modules).

You can configure I/O points to be updated in the process image every scan cycle or when a specific event interrupt occurs. You can also configure an I/O point to be excluded from process image updates. For example, your process might only need certain data values when an event such as a hardware interrupt occurs. By configuring the process image update for these I/O points to be associated with a partition that you assign to a hardware interrupt OB, you avoid having the CPU update data values unnecessarily every scan cycle when your process does not need a continual update.

For controlling whether your process updates I/O points automatically on every scan cycle, or upon the triggering of events, the S7-1200 G2 provides 32 process image partitions. The first process image partition, PIP0, is designated for I/O that is to be automatically updated every scan cycle, and is the default assignment. You can use the remaining partitions, PIP1 through PIP31, for assigning I/O process image updates to various interrupt events. You assign I/O to process image partitions in Device Configuration and you assign process image partitions to interrupt events when you create interrupt OBs [\(Page 106\)](#) or edit OB properties [\(Page 106\)](#).

By default, when you insert a module in the device view, STEP 7 sets its I/O process image update to "Automatic update". For I/O configured for "Automatic update", the CPU handles the data exchange between the module and the process image area automatically during every scan cycle.

To assign digital or analog points to a process image partition, or to exclude I/O points from process image updates, follow these steps:

1. View the Properties tab for the appropriate device in Device configuration.
2. Expand the selections under "General" as necessary to locate the desired I/O points.
3. Select "I/O addresses".
4. Optionally select a specific OB from the "Organization block" drop-down list.
5. From the "Process image" drop-down list, change "Automatic update" to a PIP from PIP1 through PIP31 or None. A selection of "None" means that you can only read from and write to this I/O using immediate instructions. To add the points back to the process image automatic update, change this selection back to "Automatic update".

You can immediately read physical input values and immediately write physical output values when an instruction executes. An immediate read accesses the current state of the physical input and does not update the process image input area, regardless of whether the point is configured to be stored in the process image. An immediate write to the physical output updates both the process image output area (if the point is configured to be stored in the process image) and the physical output point. Append the suffix ":P" to the I/O address if you want the program to immediately access I/O data directly from the physical point instead of using the process image.

NOTE**Use of process image partitions**

If you assign I/O to one of the process image partitions PIP1 - PIP31, and do not assign an OB to that partition, then the CPU never updates that I/O to or from the process image. Assigning I/O to a PIP that does not have a corresponding OB assignment is the same as assigning the process image to "None".

You can read a physical input directly with an immediate read instruction, or write to the physical output with an immediate write instruction. The CPU does not update the process image.

The CPU supports distributed I/O for PROFINET [\(Page 220\)](#) networks.

5.4.3 Startup configuration and processing

Startup configuration

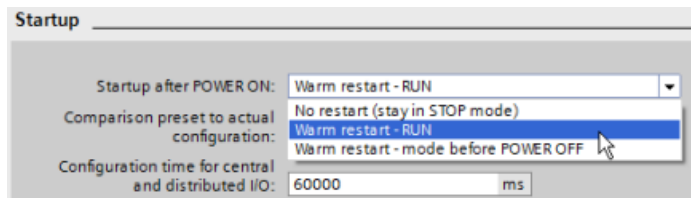
The CPU supports a warm restart for entering the RUN mode. The CPU initializes all non-retentive system and user data at warm restart, and retains the values of all retentive user data.

Warm restart does not include a memory reset. A memory reset clears all work memory, clears retentive and non-retentive memory areas, copies load memory to work memory, and sets outputs to the configured "Reaction to CPU STOP". A memory reset does not clear the diagnostics buffer or the permanently saved values of the IP address.

You can configure the "startup after POWER ON" setting of the CPU. This configuration item appears under the "Device configuration" for the CPU under "Startup". Upon powering up, the CPU performs a sequence of power-up diagnostic checks and system initialization. During system initialization, the CPU deletes all non-retentive bit (M) memory and resets all non-retentive DB contents to the initial values from load memory. The CPU retains retentive bit (M) memory and retentive DB contents and then enters the appropriate operating mode. Certain detected errors prevent the CPU from entering the RUN mode. The CPU supports the following configuration choices:

- No restart (stay in STOP mode)
- Warm restart - RUN

- Warm restart - mode prior to POWER OFF



NOTICE

Risks associated with repairable faults

The CPU can enter STOP mode due to repairable faults, such as the following:

- Failure of a replaceable signal module
- Temporary faults, such as power line disturbance or erratic power up event

Such conditions can result in property damage.

If you have configured the CPU to "Warm restart - mode prior to POWER OFF", the CPU goes to the operating mode that the CPU was in prior to the loss of power or fault. If the CPU was in STOP mode at the time of power loss or fault, the CPU goes to STOP mode on power up. The CPU stays in STOP mode until the CPU receives a command to go to RUN mode. If the CPU was in RUN mode at the time of power loss or fault, the CPU goes to RUN mode on the next power up. The CPU goes to RUN mode providing the CPU detects no errors that would inhibit a transition to RUN mode.

Configure CPUs that you intend to operate independently of a STEP 7 connection to "Warm restart - RUN". This startup mode sets the CPU to return to RUN mode on the next power cycle.

Startup processing

See Execution of the user program ([Page 101](#)) for the processing sequence during startup.

Each startup OB includes startup information that helps you determine the validity of retentive data and the time-of-day clock. You can program instructions inside the startup OBs to examine these startup values and to take appropriate action.

The CPU also performs the following tasks during the startup processing:

- Interrupts are queued but not processed during the startup phase
- No cycle time monitoring is performed during the startup phase
- Configuration changes to HSC (high-speed counter), PTO (pulse train output), and PtP (point-to-point communication) modules can be made in startup
- Actual operation of HSC, PTO, and point-to-point communication modules only occurs in RUN

After the execution of the startup OBs finishes, the CPU goes to RUN mode and processes the control tasks in a continuous scan cycle.

Changing the operating mode

You can use the "STOP" or "RUN" commands (Page 315) from the online tools of the TIA Portal to change the current operating mode. You can also include an STP instruction in your program to change the CPU to STOP mode. Other tools provide a means to change the operating mode as well.

5.4.4 Processing the scan cycle in RUN mode

For each scan cycle, the CPU performs processing as described in Execution of the user program (Page 101).

The CPU handles interrupt events that are enabled according to priority in the order in which they occur. For interrupt events, the CPU reads the inputs, executes the OB, and then writes the outputs, using the associated process image partition (PIP), if applicable.

The system guarantees that the scan cycle will be completed in a time period called the maximum cycle time; otherwise a time error event is generated.

- Each scan cycle begins by retrieving the current values of the digital and analog outputs from the process image and then writing them to the physical outputs of the CPU, SB, and SM modules configured for automatic I/O update (default configuration). When a physical output is accessed by an instruction, both the output process image and the physical output itself are updated.
- The scan cycle continues by reading the current values of the digital and analog inputs from the CPU, SB, and SMs configured for automatic I/O update (default configuration), and then writing these values to the process image. When a physical input is accessed by an instruction, the value of the physical input is accessed by the instruction, but the input process image is not updated.
- After reading the inputs, the user program is executed from the first instruction through the end instruction. This includes all the program cycle OBs plus all their associated FCs and FBs. The program cycle OBs are executed in order according to the OB number with the lowest OB number executing first.

Communications processing occurs periodically throughout the scan, possibly interrupting user program execution

(<https://support.industry.siemens.com/cs/de/en/view/59193558/158758826123>).

Self-diagnostic checks include periodic checks of the system and the I/O module status checks.

Interrupts can occur during any part of the scan cycle, and are event-driven. When an event occurs, the CPU interrupts the scan cycle and calls the OB that was configured to process that event. After the OB finishes processing the event, the CPU resumes execution of the user program at the point of interruption.

5.4.5 Organization blocks (OBs)

Organization blocks (OBs) control the execution of the user program.

The program cycle OB contains your main program. You can include more than one program cycle OB in your user program. During RUN mode, the program cycle OBs execute at the lowest priority level (Page 123) and can be interrupted by all other event types. The CPU executes the program cycle OBs in a continuous cycle known as the "program cycle" or "scan cycle". This cyclic processing is the normal type of processing used for programmable logic controllers. For many applications, the entire user program is located in a single program cycle OB.

Specific events in the CPU trigger the execution of other organization blocks. OBs cannot call each other. The startup OB runs when you start the CPU. It does not interrupt the program cycle OB. The CPU executes the startup OB before going to RUN mode.

Other OBs, called interrupt OBs, run when associated events or errors occur. These OBs interrupt the execution of the program cycle OBs.

An FC or FB cannot call an OB. Only an event such as a diagnostic interrupt or a time delay can start the execution of an OB. The CPU handles OBs according to their respective priority classes (Page 123), with higher priority OBs executing before lower priority OBs.

5.4.5.1 Program cycle OB

Program cycle OBs execute cyclically while the CPU is in RUN mode. The main block of the program is a program cycle OB. This is where you place the instructions that control your program and where you call additional user blocks. You can have multiple program cycle OBs, which the CPU executes in numerical order. Main (OB 1) is the default.

Program cycle events

The program cycle event happens once during each program cycle (or scan). During the program cycle, the CPU writes the outputs, reads the inputs and executes program cycle OBs. The program cycle event is required and is always enabled. You might have no program cycle OBs, or you might have multiple program cycle OBs. After the program cycle event occurs, the CPU executes the lowest numbered program cycle OB (usually "Main" OB 1). The CPU executes the other program cycle OBs sequentially (in numerical order) within the program cycle. Program execution is cyclical such that the program cycle event occurs at the following times:

- When the last startup OB finishes execution
- When the last program cycle OB finishes execution

You can delay the next program cycle after the program cycle OB finishes by configuring a minimum cycle time in the device configuration

Table 5-1 Start information for a program cycle OB

Input	Data type	Description
Initial_Call	Bool	True for initial call of the OB
Remanence	Bool	True if retentive data are available

5.4.5.2 Startup OB

Startup OBs execute one time when the operating mode of the CPU changes from STOP to RUN, including powering up in the RUN mode and in commanded STOP-to-RUN transitions. After completion, the main "Program cycle" begins executing. Refer to "Startup processing" in Startup configuration and processing ([Page 103](#))

The Startup OBs support the following startup data bits:

Table 5-2 Startup locations supported by the startup OB

Input	Data Type	Description
LostRetentive	Bool	This bit is true if the retentive data storage areas have been lost
LostRTC	Bool	This bit is true if the time-of-day clock (real-time clock) has been lost

5.4.5.3 Time delay interrupt OB

Time delay interrupt OBs execute after a time delay that you configure.

Time delay interrupt events

You configure time delay interrupt events to occur after a specified delay time has expired from the beginning of execution of the SRT_DINT instruction. You assign the delay time with the SRT_DINT instruction. The time delay events interrupt the program cycle to execute the corresponding time delay interrupt OB. You can attach only one time delay interrupt OB to a time delay event. The CPU supports 20 time delay events.

Table 5-3 Start information for a time delay interrupt OB

Input	Data type	Description
Sign	Word	Identifier passed to triggering call of SRT_DINT

5.4.5.4 Cyclic interrupt OB

Cyclic interrupt OBs execute at a specified interval. You can configure up to a total of 20 cyclic interrupt events, with one OB corresponding to each cyclic interrupt event.

Cyclic interrupt events

The cyclic interrupt events allow you to configure the execution of an interrupt OB at a configured cycle time. You configure the initial cycle time when you create the cyclic interrupt OB. A cyclic event interrupts the program cycle and executes the corresponding cyclic interrupt OB. Note that the cyclic interrupt event is at a higher priority class than the program cycle event.

You can attach only one cyclic interrupt OB to a cyclic event.

You can assign a phase shift to each cyclic interrupt so that the execution of cyclic interrupts can be offset from one another by the phase offset amount. For example, if you have a 5 ms cyclic event and a 10 ms cyclic event, every ten milliseconds both events occur at the same moment. If you phase shift the 5 ms event by 1 to 4 ms and the 10 ms event by 0 ms, then the two events do not occur at the same moment.

The default phase offset is 0. To change the initial phase shift, or to change the cyclic time for a cyclic event, follow these steps:

1. Right-click the cyclic interrupt OB in the project tree.
2. Select "Properties" from the context menu.
3. Click "Cyclic interrupt" from the "Cyclic interrupt [OB 30]" dialog, and enter the new initial values.

The maximum phase offset is 6000000 microseconds (6 seconds) or the maximum Cyclic time, whichever is smaller.

You can also query and change the cycle time and the phase shift from your program using the Query cyclic interrupt (QRY_CINT) and Set cyclic interrupt (SET_CINT) instructions. Cycle time and phase shift values set by the SET_CINT instruction do not persist through a power cycle or a transition to STOP mode; cycle time and phase shift values return to the initial values following a power cycle or a transition to STOP. The CPU supports a total of 20 cyclic interrupt events.

Table 5-4 Start information for cyclic interrupt OB

Name	Data type	Meaning
Initial_Call	BOOL	=TRUE in the first call of this OB • At the transition from STOP or HOLD to RUN • After reloading
Event_Count	INT	Number of discarded cyclic interrupt events since the last start of this OB

5.4.5.5 Hardware interrupt OB

Hardware interrupt OBs execute when the relevant hardware event occurs. A hardware interrupt OB interrupts normal cyclic program execution in reaction to a signal from a hardware event.

Hardware interrupt events

Changes in the hardware, such as a rising or falling edge on an input point, or an HSC (High Speed Counter) event trigger hardware interrupt events. The S7-1200 G2 supports hardware interrupt OBs to respond to hardware interrupt events.

You enable the hardware events in the device configuration, and assign an OB for an event in the device configuration or with an ATTACH instruction in the STEP 7 program. The CPU supports several hardware interrupt events. The CPU model and the number of input points determine the exact events that are available.

Limits on hardware interrupt events are as follows:

Edges:

- One for each CPU and SB digital input
- Additional hardware interrupt events are possible from distributed I/O depending on the device and submodules that you use.

HSC events:

- CV=PV: maximum of 8
- Direction changed: maximum of 8
- External reset: maximum of 8

Table 5-5 Start information for a hardware interrupt OB

Input	Data type	Description
LADDR	HW_IO	Hardware identifier of the module that triggered the hardware interrupt
USI	WORD	User structure identifier (16#0001 to 16#FFFF), reserved for future use
IChannel	USINT	Number of the channel that triggered the interrupt
EventType	BYTE	Identifier for the module-specific event type associated with the event triggering the interrupt, for example falling edge or rising edge.

Table 5-6 Bits in EventType based on module and process event

Module / Sub-module	Value	Process event
Onboard I/O from CPU, SB, or distributed I/O	16#0	Rising edge
	16#1	Falling edge
HSC	16#0	HSC CV=RV1
	16#1	HSC direction changed
	16#2	HSC reset

5.4.5.6 Time error interrupt OB

If configured, the time error interrupt OB (OB 80) executes when either the scan cycle exceeds the maximum cycle time or a time error event occurs. If triggered, it executes, interrupting normal cyclic program execution or any event OB at priority 21 or lower.

The occurrence of either of these events generates a diagnostics buffer entry describing the event. The diagnostics buffer entry is generated regardless of the existence of the time error interrupt OB.

Time error interrupt events

The occurrence of any of several different time error conditions results in a time error event:

- Scan cycle exceeds maximum cycle time

The "maximum cycle time exceeded" condition results if the program cycle does not complete within the specified maximum scan cycle time. See the topic Monitoring and configuring the cycle time (Page 126) for more information.

- CPU cannot start requested OB because a second time interrupt (cyclic or time-delay) starts before the CPU finishes execution of the first interrupt OB

- Queue overflow occurred

The "queue overflow occurred" condition results if the interrupts are occurring faster than the CPU can process them. The CPU limits the number of pending (queued) events by using a different queue for each event type. If an event occurs when the corresponding queue is full, the CPU generates a time error event.

All time error events trigger the execution of the time error interrupt OB if it exists. If the time error interrupt OB does not exist, then the following conditions determine the CPU behavior:

- If a time error interrupt OB has never been downloaded to the CPU, the CPU ignores the first scan timeout condition and remains in RUN mode. If a second scan timeout condition occurs in the same program scan (two times the maximum cycle time value), the CPU generates a diagnostic buffer entry and transitions to STOP mode.
- If the time error interrupt OB has previously been downloaded, but has since been deleted, the CPU transitions to STOP mode if a time error event occurs, because the CPU cannot find the time error OB.

The user program can extend the program cycle execution time up to ten times the configured maximum cycle time by executing the RE_TRIGR instruction to restart the cycle time monitor. However, if two "maximum cycle time exceeded" conditions occur within the same program cycle without resetting the cycle timer, then the CPU transitions to STOP, regardless of whether the time error interrupt OB exists. See the topic Monitoring and configuring the cycle time (Page 126).

Time error interrupt OB includes start information that helps you determine which event and OB generated the time error. You can program instructions inside the OB to examine these start values and to take appropriate action.

Table 5-7 Start information for the time error OB (OB 80)

Input	Data type	Description
Fault_ID	BYTE	16#01: Cycle time exceeded 16#02: The requested OB is still being processed. 16#05: Expired time interrupt due to time jump 16#06: Expired time interrupt upon re-entry into RUN after HOLD

Input	Data type	Description
		16#07: Overflow of the OB request buffer for the current priority class 16#08: Isochronous mode interrupt - time error 16#09: Interrupt loss due to high interrupt load 16#0B: Technology synchronization interrupt - time error 16#0C: (only for S7-1500 R/H CPUs) cycle time exceeded for the second time
Csg_OBnr	OB_ANY	Number of the OB which was being executed when the error occurred
Csg_Prio	UINT	Priority of the OB causing the error

See topic Organization blocks (OBs) [\(Page 106\)](#) for instructions on adding OBs to your project.

5.4.5.7 Diagnostic error interrupt OB

The diagnostic error interrupt OB executes when the CPU detects a diagnostic error, or if a diagnostics-capable module recognizes an error and you have enabled the diagnostic error interrupt for the module. The diagnostic error interrupt OB interrupts the normal cyclic program execution. You can include an STP instruction in the diagnostic error interrupt OB to put the CPU in STOP mode if you desire your CPU to enter STOP mode upon receiving this type of error.

If you do not include a diagnostic error interrupt OB in your program, the CPU ignores the error and stays in RUN mode.

Diagnostic error events

PROFINET, local analog, and some local digital devices are capable of detecting and reporting diagnostic errors. The occurrence or removal of any of several different diagnostic error conditions results in a diagnostic error event. Standard CPUs and modules can generate the following diagnostic errors:

- No user power
- High limit exceeded
- Low limit exceeded
- Wire break
- Short circuit

Distributed devices can generate additional diagnostic errors.

Diagnostic error events trigger the execution of the diagnostic error interrupt OB (OB 82) if it exists. If it does not exist, then the CPU ignores the error.

See topic Organization blocks (OBs) [\(Page 106\)](#) for instructions on adding an OB to your project.

NOTE**Diagnostic errors for multi-channel local analog devices**

The diagnostic error interrupt OB can process only one channel's diagnostic error at a time. If two channels of a multi-channel device have an error, then the second error only triggers the diagnostic error interrupt OB under the following conditions: the first channel error clears, the execution of the diagnostic error interrupt OB that the first error triggered is complete, and the second error still exists.

The diagnostic error interrupt OB includes startup information that helps you determine whether the event is due to the occurrence or removal of an error, and the device and channel which reported the error. You can program instructions inside the diagnostic error interrupt OB to examine these startup values and to take appropriate action.

NOTE

If the outgoing event leaves the submodule with no pending diagnostics, the Diagnostic error OB start information references the submodule as a whole (16#8000), even if the source of the event was a specific channel.

Table 5-8 Startup information for the diagnostic error interrupt OB

Input	Data type	Description
Istate	WORD	IO state of the device: • Bit 0 = 1 if the configuration is correct, and = 0 if the configuration is no longer correct. • Bit 4 = 1 if an error is present (such as a wire break). (Bit 4 = 0 if there is no error.) • Bit 5 = 1 if the configuration is not correct, and = 0 if the configuration is correct again. • Bit 7 = 1 if an I/O access error has occurred. Refer to LADDR for the hardware identifier of the I/O with the access error. (Bit 6 = 0 if there is no error.) Status of the hardware object: • Bit 0: Good • Bit 1: Deactivated • Bit 2: Maintenance required • Bit 3: Maintenance demanded • Bit 4: Error • Bit 5: Not available • Bit 6: Qualified • Bit 7: Not available

Input	Data type	Description
		- Bits 8 to 14: Reserved (always "0") - Bit 15: Network / hardware fault If bit 4 = 1 or bit 5 = 1: - Bit 15 = 0: Network error - Bit 15 = 1: Hardware error
LADDR	HW_ANY	Hardware identifier of the device or functional unit that reported the error ¹
Channel	UINT	Channel number
MultiError	BOOL	TRUE if more than one error is present

¹ The LADDR input contains the hardware identifier of the device or functional unit which returned the error. The hardware identifier is assigned automatically when components are inserted in the device or network view and appears in the System constants tab of PLC tags. A name is also assigned automatically for the hardware identifier. These entries in the System constants tab of the PLC tags cannot be changed.

5.4.5.8 Pull or plug of modules OB

The "Pull or plug of modules" OB executes when a configured and non-disabled distributed I/O module or submodule generates an event related to inserting or removing a module.

Pull or plug of modules event

The following conditions generate a pull or plug of modules event:

- Someone removes or inserts a configured module
- A configured module is not physically present in an expansion rack
- An incompatible module is in an expansion rack that does not correspond to the configured module
- A compatible module for a configured module is in an expansion rack, but the configuration does not allow substitutes
- A module or submodule has parameterization errors

If you have not programmed this OB, the CPU remains in RUN mode when any of these conditions occur with a configured and non-disabled distributed I/O module.

Regardless of whether you have programmed this OB, the CPU changes to STOP mode when any of these conditions occur with a module in the local rack.

Table 5-9 Start information for pull or plug of modules OB

Input	Data type	Description
LADDR	HW_IO	Hardware identifier
Event_Class	Byte	16#38: module inserted 16#39: module removed
Fault_ID	Byte	Fault identifier

Input	Data type	Description
		For event class 16#38: • 54: Submodule inserted, which conforms to the parameterized submodule • 55: Submodule inserted, which does not conform to the submodule parameter assignment • 56: Submodule inserted, but error in module parameter assignment • 57: Submodule inserted, but with a fault or maintenance issue • 58: Submodule access error remedied For event class 16#39 • 51: Module removed • 54: Submodule removed

5.4.5.9 Rack or station failure OB

The "Rack or station failure" OB executes when the CPU detects the failure or communication loss of a distributed rack or station.

Rack or station failure event

The CPU generates a rack or station failure event when it detects one of the following:

- The failure of a DP master system or of a PROFINET IO system (in the case of either an incoming or an outgoing event).
- The failure of a DP slave or of an IO device (in the case of either an incoming or an outgoing event)
- Failure of some of the submodules of a PROFINET I-device

If you have not programmed this OB, the CPU remains in RUN mode when any of these conditions occur.

Table 5-10 Start information for rack or station failure OB

Input	Data type	Description
LADDR	HW_Device	Hardware identifier
Event_Class	Byte	16#38: outgoing event 16#39: incoming event
Fault_ID	Byte	Fault identifier (possible values: 16#C3, 16#C4, 16#C9, 16#CA, 16#CB, 16#CC, 16#CD, 16#CE, 16#CF, 16#F8, 16#F9)

The following table shows which event caused the start of OB 86.

ev_class 16# ...	fault_id 16# ...	Meaning
39	C3	Failure of a DP master system
39/38	C4	Failure/return of a DP slave
39	CA	Failure of a PROFINET IO system
39/38	CB	Failure/return of a PROFINET IO device
38	CC	Return of a PROFINET IO device with fault or maintenance

ev_class 16# ...	fault_id 16# ...	Meaning
38	CD	Return of a PROFINET IO device, deviation between preset/actual configuration
38	CE	Return of a PROFINET IO device, error in module configuration
39/38	F8	Failure/return of some of the submodules of a PROFINET I-device
38	F9	Return of some of the submodules of a PROFINET I-device with a device configuration difference

5.4.5.10 Time of day OB

Time of day OBs execute based on configured clock time conditions. The CPU supports up to 20 time of day OBs.

Time of day events

You can configure a time of day interrupt event to occur once on a specified date or time or cyclically with one of the following cycles:

- Every minute: The interrupt occurs every minute.
- Hourly: The interrupt occurs every hour.
- Daily: The interrupt occurs every day at a specified time (hour and minute).
- Weekly: The interrupt occurs every week at a specified time on a specified day of the week (for example, every Tuesday at 4:30 in the afternoon).
- Monthly: The interrupt occurs every month at a specified time on a specified day of the month. The day number must be between 1 and 28, inclusive.
- Every end of month: The interrupt occurs on the last day of every month at a specified time.
- Yearly: The interrupt occurs every year on the specified date (month and day). You cannot specify a date of February 29.

Table 5-11 Start information for a time of day event OB

Input	Data type	Description
CaughtUp	Bool	OB call is caught up because time was set forward
SecondTime	Bool	OB call is started a second time because time was set backward

5.4.5.11 Synchronous cycle OB

IRT (Isochronous Realtime) is a transmission method that can synchronize PROFINET devices with very high accuracy. You can operate I/O modules in distributed PROFINET I/O systems isochronously, for example, ET 200SP and ET 200MP distributed I/O systems. Both the I/O modules and the interface modules of the I/O systems must support isochronous mode.

The Synchronous cycle interrupt OB uses an isochronous mode interrupt to trigger the start of subprograms isochronously to the PROFINET send clock.

Refer to Cycle time and communication load (Page 128) for considerations of how higher priority OBs affect the main scan cycle.

Table 5-12 Start information for Synchronous cycle OB

Input	Data type	Meaning
Initial_Call	BOOL	TRUE = the first call of this OB during transition from STOP to RUN
PIP_Input	BOOL	Always FALSE. The program must call the SYNC_PI instruction to update the corresponding process image partition of the inputs.
PIP_Output	BOOL	Always FALSE. The program must call the SYNC_PO instruction to update the corresponding process image partition.
IO_System	USINT	Number of the distributed I/O system triggering the interrupt
Event_Count	INT	= n: Number of lost cycles = -1: An unknown number of cycles has been lost (for example, because cycle has changed)
SyncCycleTime	LTIME	Configured cycle time of the Synchronous cycle OB

5.4.5.12 Status OB

Status OBs execute if a PNIO slave triggers a status interrupt. This might be the case if a component (module or rack) of a PNIO slave changes its operating mode, for example from RUN to STOP.

Status events

For detailed information on events that trigger a status interrupt, refer to the manufacturer's documentation for the PNIO device.

Table 5-13 Start information for status OB

Input	Data type	Description
LADDR	HW_IO	Hardware identifier
Slot	UInt	Slot number
Specifier	Word	Alarm specifier

5.4.5.13 Update OB

Update OBs execute if a PNIO slave triggers an update interrupt.

Update events

For detailed information on events that trigger an update interrupt, refer to the manufacturer's documentation for the PNIO slave.

Table 5-14 Start information for update OB

Input	Data type	Description
LADDR	HW_IO	Hardware identifier
Slot	UInt	Slot number
Specifier	Word	Alarm specifier

5.4.5.14 Profile OB

Profile OBs execute if a DPV1 or PNIO slave triggers a profile-specific interrupt.

Profile events

For detailed information on events that trigger a profile interrupt, refer to the manufacturer's documentation for the DPV1 or PNIO slave.

Table 5-15 Start information for profile OB

Input	Data type	Description
LADDR	HW_IO	Hardware identifier
Slot	UInt	Slot number
Specifier	Word	Alarm specifier

5.4.5.15 MC-Servo and MC-Interpolator OB

STEP 7 creates the read-only MC-Servo and MC-Interpolator OBs automatically when you create a motion technology object and set the drive interface to be "Analog drive connection" or "PROFIDrive". You do not need to edit any OB properties or create this OB directly. The CPU uses these OBs for closed loop control. Refer to the STEP 7 Information System for further details.

The MC Servo OB uses a system-defined PIP with the name "PIP OB Servo".

Table 5-16 Start information for MC-Servo OB

Input	Data type	Description
Initial_Call	BOOL	TRUE indicates first call of this OB on transition from STOP to RUN
PIP_Input	BOOL	TRUE indicates the associated process image input is up to date.
PIP_Output	BOOL	TRUE indicates that the CPU transferred the associated process image output to the outputs in good time after the last cycle.

Input	Data type	Description
IO_System	USINT	Number of the distributed I/O system triggering the interrupt
Event_Count	INT	n: number of lost cycles -1: unknown number of cycles lost (for example, because cycle has changed)
Synchronous	BOOL	TRUE: The MC-Servo [OB91] is called synchronously with a bus system

Table 5-17 Start information for MC-Interpolator OB

Input	Data type	Description
Initial_Call	BOOL	TRUE indicates first call of this OB on transition from STOP to RUN
PIP_Input	BOOL	TRUE indicates the associated process image input is up to date.
PIP_Output	BOOL	TRUE indicates that the CPU transferred the associated process image output to the outputs in good time after the last cycle.
IO_System	USINT	Number of the distributed I/O system triggering the interrupt
Event_Count	INT	n: number of lost cycles -1: unknown number of cycles lost (for example, because cycle has changed)
Reduction	UInt	Reduction ratio of MC-Interpolator [OB92] to MC-Servo [OB91]

5.4.5.16 MC-PreInterpolator

The organization block MC_PreInterpolator [OB68] can be programmed and is called in the application cycle configured at the MC_Servo (Page 117). The MC_PreInterpolator is called directly before the MC_Interpolator.

Via the organization block, you can read out the configured application cycle.

Structure of the start information

Optimized start information:

Name	Data type	Meaning	
Initial_Call	BOOL	TRUE	In the first call of this OB after the CPU is switched on
PIP_Input	BOOL	TRUE	The associated process image input is up-to-date.
PIP_Output	BOOL	TRUE	The associated process image output was transferred to the outputs in time after the last cycle.
IO_System	USINT	Number of the distributed I/O system triggering the interrupt	
Event_Count	INT	n	Number of lost cycles
		-1	An unknown number of cycles has been lost, e.g. because the cycle has changed.
Reduction	UINT	Reduction ratio of MC_Interpolator to MC_Servo	
CycleTime	UDINT	Display of the application cycle configured for the MC_Interpolator in ns	

5.4.5.17 MC-PreServo

You can program the MC-PreServo OB to contain program logic for the STEP 7 program to execute directly before the MC-Servo OB executes.

MC-PreServo events

The MC-PreServo OB allows you to read out the configured application cycle information in microseconds.

Table 5-18 Start information for MC-PreServo OB

Input	Data type	Description
Initial_Call	BOOL	TRUE indicates first call of this OB on transition from STOP to RUN
PIP_Input	BOOL	TRUE indicates the associated process image input is up to date.
PIP_Output	BOOL	TRUE indicates that the CPU transferred the associated process image output to the outputs in good time after the last cycle.
IO_System	USINT	Number of the distributed I/O system triggering the interrupt
Event_Count	INT	n: number of lost cycles -1: unknown number of cycles lost (for example, because cycle has changed)
Synchronous	BOOL	Reserved
CycleTime	UDINT	Display of the application cycle configured for the MC-Servo OB in microseconds

5.4.5.18 MC-PostServo

You can program the MC-PostServo OB to contain program logic for the STEP 7 program to execute directly after the MC-Servo OB executes.

MC-PostServo events

The MC-PostServo OB allows you to read out the configured application cycle information in microseconds.

Table 5-19 Start information for MC-PostServo OB

Input	Data type	Description
Initial_Call	BOOL	TRUE indicates first call of this OB on transition from STOP to RUN
PIP_Input	BOOL	TRUE indicates the associated process image input is up to date.
PIP_Output	BOOL	TRUE indicates that the CPU transferred the associated process image output to the outputs in good time after the last cycle.
IO_System	USINT	Number of the distributed I/O system triggering the interrupt
Event_Count	INT	n: number of lost cycles -1: unknown number of cycles lost (for example, because cycle has changed)
Synchronous	BOOL	Reserved
CycleTime	UDINT	Display of the application cycle configured for the MC-Servo OB in microseconds

5.4.5.19 MC-LookAhead

STEP 7 creates the read-only MC_LookAhead OB automatically when you create a kinematics technology object. MC_LookAhead calculates the motion preparation of the kinematics technology object.

STEP 7 creates only one MC_LookAhead OB for all kinematics.

MC_LookAhead prepares the jobs of the job sequence in advance. In this way, less time is required for motion preparation in the MC_Interpolator organization block [\(Page 117\)](#) and you can set a shorter application cycle of the MC_Servo organization block [\(Page 117\)](#).

Downloading in RUN mode [\(Page 340\)](#) increases the CPU time required to prepare the motion jobs in the job sequence.

Block call and priority

MC_LookAhead is triggered by MC_Interpolator.

You configure the priority of the MC_LookAhead in the properties of the organization block under "General > Attributes > Priority". You can set values from 15 to 16 (default setting 15) for the priority. The priority of MC_LookAhead must be lower than the priority of MC_Interpolator.

Process response

Overflows can occur in the program scan cycle. Note the following response to overflows:

- The CPU tolerates a maximum of three consecutive MC_Interpolator overflows.
- The execution of an MC_Interpolator can only be interrupted by an MC_Servo call.

If more overflows or interruptions occur, the CPU transitions to STOP mode.

5.4.5.20 Programming error OB

The programming error OB executes if a programming error occurs during the processing of an instruction of the STEP 7 program. The programming error OB is processed according to its priority (Page 123).

You can handle programming errors locally using the GET_ERROR or GET_ERR_ID instructions within a program block. Otherwise, the CPU performs global error handling.

With global error handling, a programming error event triggers the execution of the programming error OB, if it exists, and the CPU stays in RUN mode. If the STEP 7 program does not include the programming error OB, the CPU goes to STOP mode when a programming error occurs.

Table 5-20 Start information for the programming error OB

Name	Data type	Meaning
BlockNr	UINT	Number of the block in which the programming error occurred
Reaction	USINT	0: Ignore errors 1: Replace incorrect value 2: Skip command 3: Programmed error handling, triggered by an array access with invalid index, for example, or by an error during parameter supply of an FC or FB
Fault_ID	BYTE	Error code (possible values: B#16#00, B#16#03, B#16#04, B#16#05, B#16#20, B#16#21, B#16#22, B#16#23, B#16#24, B#16#25, B#16#26, B#16#27, B#16#28, B#16#29, B#16#2C, B#16#30, B#16#31, B#16#32, B#16#33, B#16#34, B#16#35, B#16#38, B#16#39, B#16#3A, B#16#3B, B#16#3C, B#16#3D, B#16#3E, B#16#3F, B#16#50, B#16#51, B#16#75, B#16#76, B#16#A1, B#16#A2)
BlockType	USINT	Type of block in which the error occurred: - OB: 1 - FC: 2 - FB: 3 - SFC: 4 - SFB: 5 - DB: 6
Area	USINT	Area in which the incorrect access occurred: - Local data: B#16#40 to 4E, 86, 87, 8E, 8F, C0 to CE - Process image input: B#16#01 - Process image output: B#16#02 - Technology DB: B#16#04 - I: B#16#81 - Q: B#16#82 - M: B#16#83 - DB: B#16#84, 85, 8A, 8B
DBNr	DB_ANY	DB no. if AREA = DB or DI

Name	Data type	Meaning
Csg_OBNr	OB_ANY	OB number
Csg_Prio	USINT	OB priority
Width	USINT	Type of access during which the error occurred: • Bit: – B#16#00 for access to the standard memory area – B#16#01 for access to the optimized memory area • Byte: B#16#01 • Word: B#16#02 • DWord: B#16#03 • LWord: B#16#04

5.4.5.21 I/O access error OB

I/O access error OBs execute when the CPU executes an instruction that references I/O that does not exist.

You can handle I/O access errors locally using the GET_ERROR or GET_ERR_ID instructions within a program block. Otherwise, the CPU performs global error handling. With global error handling, an I/O access error event triggers the execution of the I/O access error OB, if it exists.

Table 5-21 Start information for the I/O access error OB

Name	Data type	Meaning
BlockNr	UINT	Number of the block in which the I/O access error occurred
Reaction	USINT	0: Ignore error, 1: Replace incorrect value, 2: Skip command
Fault_ID	BYTE	Error code: • B#16#42: I/O access error, reading • B#16#43: I/O access error, writing
BlockType	USINT	Type of block in which the error has occurred: • OB: 1 • FC: 2 • FB: 3 • SFC: 4 • SFB: 5 • DB: 6
Area	USINT	Identifier for the range in which the incorrect access occurred: • B#16#01: Direct access to input • B#16#02: Direct access to output • B#16#81: Access to process image input • B#16#82: Access to process image output
DBNr	DB_ANY	not user-relevant

Name	Data type	Meaning
Csg_OBNr	OB_ANY	OB number causing the I/O access error
Csg_Prio	USINT	OB priority that causes the I/O access error
Width	USINT	Type of access during which the error occurred: • Bit: B#16#00 • Byte: B#16#01 • Word: B#16#02 • DWord: B#16#03 • LWord: B#16#04

5.4.5.22 Event execution priorities and queuing

Events control CPU processing. An event triggers an interrupt OB to be executed. You can specify the interrupt OB for an event during the creation of the block, during the device configuration, or with an ATTACH or DETACH instruction. Some events happen on a regular basis like the program cycle or cyclic events. Other events happen only a single time, like the startup event and time delay events. Some events happen when the hardware triggers an event, such as an edge event on an input point or a high speed counter event. Events like the diagnostic error and time error event only happen when an error occurs. The event priorities and queues are used to determine the processing order for the event interrupt OBs.

The CPU processes events in order of priority where 1 is the lowest priority and 26 is the highest priority. You can assign a priority class to an OB in the attributes of the OB properties.

Interruptible OBs

OBs (Page 106) execute in priority order of the events that trigger them.

If an OB is executing and a higher priority event occurs before the OB completes its execution, the running OB is interrupted to allow the higher-priority event OB to run. The higher-priority event runs, and at its completion, the OB that was interrupted continues. When multiple events occur while an interruptible OB is executing, the CPU processes those events in priority order.

Consider the case where interrupt events trigger a cyclic OB and a time delay OB. In this example, the time delay OB (OB 201) has no process image partition assignment (Page 101) and executes at priority 4. The cyclic OB (OB 200) has a process image partition assignment of PIP1 and executes at priority 2. The following illustration shows interruptible OB execution mode:

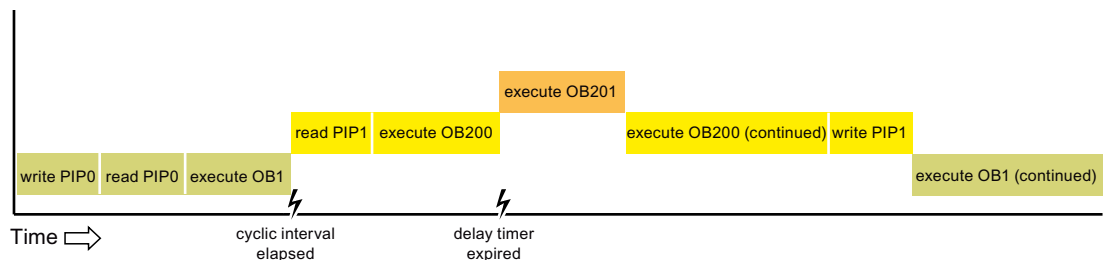
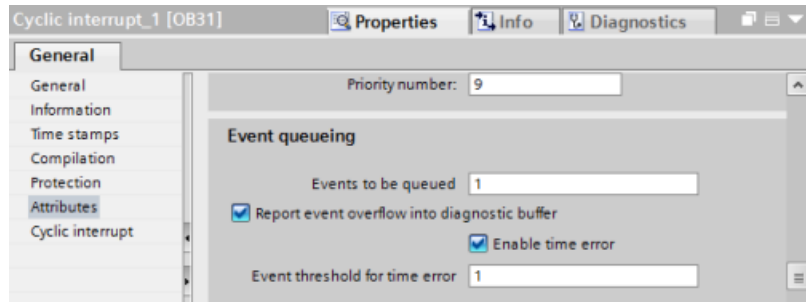


Figure 5-1 Interruptible OB execution

Understanding event execution priorities and queuing

The CPU limits the number of pending (queued) events from a single source, using a different queue for each event type. Upon reaching the limit of pending events for a given event type, the next event is lost. You can use a time error interrupt OB (Page 110) to respond to queue overflows.

Note that STEP 7 allows you to configure some specific event queuing parameters for the Cyclic interrupt OB and the Time of day OB.



For further information on CPU overload behavior and event queueing, refer to the "CPU overload behavior

(https://docs.tia.siemens.cloud/access?ft:originId=./39470090251/39481356555_enUS.htm&ft:clusterId./39470090251/39481356555.htm)" topic. The TIA Portal Information System does not have a specific S7-1200 G2 topic on overload behavior and event queueing.

Each CPU event has an associated priority. In general, the CPU services events in order of priority (highest priority first). The CPU services events of the same priority on a "first-come, first-served" basis.

Table 5-22 OB events

Event	Quantity allowed	Default OB priority
Program cycle	1 program cycle event ¹ Multiple OBs allowed	1
Startup	1 startup event ¹ Multiple OBs allowed	1
Time delay	Up to 20 time events 1 OB per event	OB 20: 3 OB 21: 4 OB 22: 5 OB 23: 6 OB 123 to OB 32767: 3
Cyclic interrupt	Up to 20 events 1 OB per event	8 to 17

¹ The startup event and the program cycle event never occur at the same time because the startup event runs to completion before the program cycle event starts.

² You can have more than 50 hardware interrupt event OBs if you use the DETACH and ATTACH instructions.

³ You can configure the CPU to stay in RUN if the scan cycle exceeds the maximum scan cycle time or you can use the RE_TRIGR instruction to reset the cycle time. However, the CPU goes to STOP mode the second time that one scan cycle exceeds the maximum scan cycle time.

⁴ Programming errors enable the program block to handle errors with GET_ERROR and GET_ERROR_ID within a program block. In the absence of these instructions, the CPU uses global error handling.

⁵ The CPU logs the first direct I/O read/write error in the diagnostics buffer and stays in RUN mode. You can access the error cause using the GET_ERROR_ID instruction.

Event	Quantity allowed	Default OB priority
Hardware interrupt	Up to 50 hardware interrupt events ² 1 OB per event, but you can use the same OB for multiple events	16
Time error	1 event (only if configured) ³	22
Diagnostic error	1 event (only if configured)	5
Pull or plug of modules	1 event	6
Rack or station failure	1 event	6
Synchronous cycle	1 event	21
Time of day	Up to 20 events	2
Status	1 event	4
Update	1 event	4
Profile	1 event	4
MC-Servo	1 event	25
MC-Interpolator	1 event	24
MC-PreServo	1 event	Same priority as MC-Servo
MC-PostServo	1 event	Same priority as MC-Servo
MC-PreInterpolator	1 event	Same priority as MC-Interpolator
MC-Lookahead	1 event	15
Programming error ⁴	1 event	7
I/O access error ⁵	1 event	7

¹ The startup event and the program cycle event never occur at the same time because the startup event runs to completion before the program cycle event starts.

² You can have more than 50 hardware interrupt event OBs if you use the DETACH and ATTACH instructions.

³ You can configure the CPU to stay in RUN if the scan cycle exceeds the maximum scan cycle time or you can use the RE_TRIGR instruction to reset the cycle time. However, the CPU goes to STOP mode the second time that one scan cycle exceeds the maximum scan cycle time.

⁴ Programming errors enable the program block to handle errors with GET_ERROR and GET_ERROR_ID within a program block. In the absence of these instructions, the CPU uses global error handling.

⁵ The CPU logs the first direct I/O read/write error in the diagnostics buffer and stays in RUN mode. You can access the error cause using the GET_ERROR_ID instruction.

In addition, the CPU recognizes other events that do not have associated OBs. The following table describes these events and the corresponding CPU actions:

Table 5-23 Additional events

Event	Description	CPU action
Max cycle time error	CPU exceeds the configured cycle time twice	The CPU logs the error in the diagnostics buffer and transitions to STOP mode.
Peripheral access error	I/O error during process image update	The CPU logs the first occurrence in the diagnostics buffer and stays in RUN mode.

Interrupt latency

The interrupt event latency (the time from notification of the CPU that an event has occurred until the CPU begins execution of the first instruction in the OB that services the event) is approximately 200 µsec, provided that a program cycle OB is the only event service routine active at the time of the interrupt event.

5.4.6 Monitoring and configuring the cycle time

The cycle time is the time that the CPU operating system requires to execute the cyclic phase of the RUN mode. The CPU provides two methods of monitoring the cycle time:

- Maximum scan cycle time
- Minimum scan cycle time

Scan cycle monitoring begins after the startup event is complete. Configuration for this feature appears under the "Device Configuration" for the CPU under "Cycle".

The CPU monitors the scan cycle. If the scan cycle time exceeds the configured maximum scan cycle time, the CPU generates an error and responds as follows:

- If the user program includes a time error interrupt OB ([Page 110](#)), then the CPU executes it.
- If the user program does not include a time error interrupt OB, then the time error event generates a diagnostic buffer entry. The CPU behavior is determined by the following:
 - If a time error interrupt OB has never been downloaded to the CPU, the CPU ignores the first scan timeout condition and remains in RUN mode. If a second scan timeout condition occurs in the same program scan (two times the maximum cycle time value), the CPU generates a diagnostic buffer entry and transitions to STOP mode.
 - If the time error interrupt OB has previously been downloaded, but has since been deleted, the CPU transitions to STOP mode if a time error event occurs, because the CPU cannot find the time error OB.

The RE_TRIGR instruction (re-trigger cycle time monitoring) allows you to reset the timer that measures the cycle time. If the elapsed time for the current program cycle execution is less than ten times the configured maximum scan cycle time, the RE_TRIGR instruction retriggers the cycle time monitoring and returns with ENO = TRUE. If not, the RE_TRIGR instruction does not retrigger the cycle time monitoring. It returns ENO = FALSE.

Typically, the scan cycle executes as fast as it can and the next scan cycle begins as soon as it completes. Depending upon the user program and communication tasks, the time period for a scan cycle can vary from scan to scan. To eliminate this variation, the CPU supports an optional minimum scan cycle time. By default, the minimum scan cycle time is enabled and is 1 ms. When enabled, the CPU delays after the execution of the program cycle OBs until the minimum scan cycle time elapses before repeating the program cycle.

In the event that the CPU completes the normal scan cycle in less time than the specified minimum cycle time, the CPU spends the additional time of the scan cycle performing runtime diagnostics and/or processing communication requests ([Page 128](#)).

In the event that the CPU does not complete the scan cycle in the specified minimum cycle time, the CPU completes the scan normally (including communication processing) and does not create any system reaction as a result of exceeding the minimum scan time. The following table defines the ranges and defaults for the cycle time monitoring functions:

Table 5-24 Range for the cycle time

Cycle time	Range (ms)	Default
Maximum scan cycle time ¹	1 to 6000	150 ms
Minimum scan cycle time ²	1 to maximum scan cycle time	1 ms

¹ The maximum scan cycle time is always enabled. Configure a cycle time between 1 ms to 6000 ms. The default is 150 ms.

² The minimum scan cycle time is 1 ms by default. If required, configure a cycle time between 1 ms and the maximum scan cycle time.

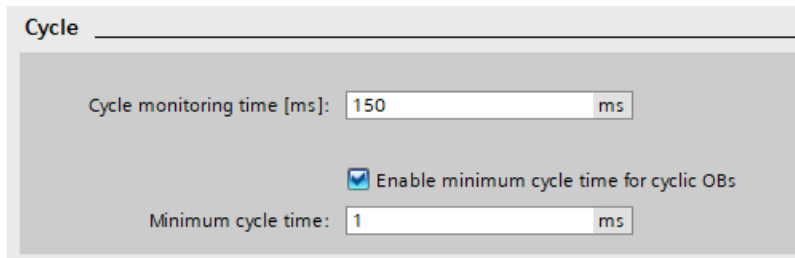
NOTE

To run as fast as possible, deselect "Enable minimum cycle time for cyclic OBs" under "Cycle > Cycle monitoring time [ms]" in Device configuration.

5.4.7 Cycle time and communication load

You use the CPU properties in the Device configuration to configure the following parameters:

- **Cycle:** You can enter a maximum scan cycle monitoring time. You can also enable and enter a minimum scan cycle time.



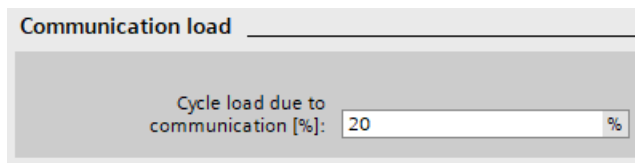
Cycle

Cycle monitoring time [ms]: 150 ms

☒ Enable minimum cycle time for cyclic OBs

Minimum cycle time: 1 ms

- **Communication load:** You can configure a percentage of the time to be dedicated for communication tasks.



Communication load

Cycle load due to communication [%]: 20 %

NOTE

Communication impact on scan cycle

Using OBs with a higher priority than the main scan cycle can cause a performance strain on the execution cycle of the CPU. To mitigate this issue, reduce the Communication load setting. more information about cycle and response times, see SIMATIC S7-1500, S7-1500R/H, ET 200SP, ET 200pro Cycle and response times

(<https://support.industry.siemens.com/cs/us/en/view/59193558/158758826123>).

NOTE

Communication priority

Communication tasks have a priority of 15. CPU events with a priority of 16 or higher can interrupt communication processing. Interrupts from other events can negatively affect communication processing during the scan cycle. You can adjust the "Cycle load due to communication" percentage to increase the portion of the scan cycle dedicated to communication processing.

For more information about the scan cycle, see Execution of the user program (Page 101)

5.4.8 CPU memory

5.4.8.1 Memory management

The CPU provides the following memory areas to store the user program, data, and configuration:

- Load memory is non-volatile storage for the user program, data and configuration. When you download a project to the CPU, the CPU first stores the program in the Load memory area. This area is located either in a SIMATIC memory card (if present) or in the CPU. The CPU maintains this non-volatile memory area through a power loss. The memory card supports a larger storage space than that built-in to the CPU.
- Work memory is volatile storage for some elements of the user project while executing the user program. The CPU copies some elements of the project from load memory into work memory. This volatile area is lost when power is removed and is restored by the CPU when power is restored. Work memory consists of two types:
 - Code work memory
 - Data work memory
- Retentive memory is non-volatile storage for a limited quantity of work memory values. The CPU uses the retentive memory area to store the values of selected user memory locations during power loss. When a power down or power loss occurs, the CPU restores these retentive values upon power up.

The size of the user program, data, and configuration is limited by the available load memory and work memory in the CPU.

To display the memory usage for a compiled program block, right-click the block in the "Program blocks" folder in the STEP 7 project tree and select "Properties" from the context menu. The Compilation properties display the load memory and work memory for the compiled block.

To display the memory usage for the online CPU, double-click "Online & diagnostics" in STEP 7, expand "Diagnostics", and select "Memory".

Representation of load memory

Load memory as represented in the Project info window includes the program blocks, technology objects, data types, and PLC tags.

Load memory as represented in Online & diagnostics includes additional objects that correspond to the project, such as project languages, certificates, and other configuration data.

Retentive memory

You can avoid data loss after power failure by marking certain data as retentive. The CPU allows you to configure the following data as retentive:

- **Bit memory (M):** You can define the size of retentive memory for bit memory in the PLC tag table or in the assignment list. Retentive bit memory always starts at M0 and runs consecutively up through a specified number of bytes. Specify this value from the PLC tag table or in the assignment list by clicking the "Retain" toolbar icon. Enter the number of M bytes to retain starting at M0.

Note: You can display an assignment list for bit memory (M) by selecting the CPU in the project tree and selecting the **Tools > Assignment list** menu command.

- **Tags of a function block (FB):** If an FB is of type "Optimized block access", then the interface editor for this FB includes a "Retain" column. In this column, you can select either "Retain", "Non-retain", or "Set in IDB" individually for each tag. When you place such an FB in the program, the instance DB that corresponds to the FB includes this "Retain" column as well. You can only change the retentive state of a tag from within the instance DB interface editor if you selected "Set in IDB" (Set in instance data block) in the Retain selection for the tag in the optimized FB.

If an FB is **not** of type "Optimized block access", then the interface editor for this FB does not include a "Retain" column. When you place such an FB in the program, the instance DB that corresponds to the FB does, however, include a "Retain" column that is available for edit. In this case, selecting the "Retain" option for any tag results in the selection of **all** tags. Similarly, deselecting the option for any tag results in the deselection of **all** tags.

To view or modify whether an FB is optimized, open the properties of the FB and select the attributes.

- **Tags of a global data block:** If you select "Optimized block access" for the attributes in the properties of the data block, you can set each tag to be retentive or not. If you do not select "Optimized block access", then all of the data block tags have the same state. The tags are either all retentive or all non-retentive.

The technical specifications for the CPUs state the retentive data allocation. The STEP 7 project version can alter the amount of retentive memory. From the PLC tag table in STEP 7 or the assignment list, click the "Retain" toolbar icon to see how much memory is available.

5.4.8.2 Notes about retentive memory

NOTE

Downloading a program does not clear or make any changes to existing values in retentive memory. If you want to clear retentive memory before a download, then reset your CPU to factory settings prior to downloading the program.

NOTE

When power failure occurs, the CPU switches off power to all expansion modules and expansion boards. This ensures that the CPU has sufficient power to save retentive data to non-volatile memory.

5.4.8.3 System and clock memory

Use the CPU properties to enable bytes for "system memory" and "clock memory". Your program logic can reference the individual bits of these functions by their tag names.

The CPU initializes these bytes on the transition from STOP mode to STARTUP mode. The bits of the clock memory change synchronously to the CPU clock throughout the STARTUP and RUN modes.

WARNING

Risks with overwriting the system memory or clock memory bits

Overwriting the system memory or clock memory bits can corrupt the data in these functions and cause your user program to operate incorrectly. Because both the clock memory and system memory are unreserved in M memory, instructions or communications can write to these locations and corrupt the data.

Avoid writing data to these locations to ensure the proper operation of these functions, and always implement an emergency stop circuit for your process or machine.

Incorrect program operation can cause damage to equipment, severe injury, or death.

System memory

You can assign one byte in M memory for system memory. The byte of system memory provides the following four bits that can be referenced by your user program by the following tag names:

- First cycle: (Tag name "FirstScan") bit is set to 1 for the duration of the first scan after the startup OB finishes. (After the execution of the first scan, the "first scan" bit is set to 0.)
- Diagnostics status changed: (Tag name: "DiagStatusUpdate") is set to 1 for one scan after the CPU logs a diagnostic event. Because the CPU does not set the "DiagStatusUpdate" bit until the end of the first execution of the program cycle OBs, your user program cannot detect if there has been a diagnostic change either during the execution of the startup OBs or the first execution of the program cycle OBs.
- Always 1 (high): (Tag name "AlwaysTRUE") bit is always set to 1.
- Always 0 (low): (Tag name "AlwaysFALSE") bit is always set to 0.

System memory bits have specific meanings, as shown in the table below:

System memory bits	
	☒ Enable the use of system memory byte
Address of system memory byte (MBx):	1
First cycle:	%M1.0 (FirstScan)
Diagnostics status changed:	%M1.1 (DiagStatusUpdate)
Always 1 (high):	%M1.2 (AlwaysTRUE)
Always 0 (low):	%M1.3 (AlwaysFALSE)

Table 5-25 System memory

7	6	5	4	3	2	1	0
Reserved Value 0				Always off Value 0	Always on Value 1	Diagnostic status indicator 1: Change 0: No change	First scan indicator 1: First scan after startup 0: Not first scan

Clock memory

You can assign one byte in M memory for clock memory. Each bit of the byte configured as clock memory generates a square wave pulse on the corresponding M memory bit. The byte of clock memory provides 8 different frequencies, from 0.5 Hz (slow) to 10 Hz (fast). You can use these bits as control bits, especially when combined with edge instructions, to trigger actions in the user program on a cyclic basis.

Clock memory bits

☒ Enable the use of clock memory byte

Address of clock memory byte (MBx):

10 Hz clock:

5 Hz clock:

2.5 Hz clock:

2 Hz clock:

1.25 Hz clock:

1 Hz clock:

0.625 Hz clock:

0.5 Hz clock:

Table 5-26 Clock memory

Bit number	7	6	5	4	3	2	1	0
Period (s)	2.0	1.6	1.0	0.8	0.5	0.4	0.2	0.1
Frequency (Hz)	0.5	0.625	1	1.25	2	2.5	5	10

Because clock memory runs asynchronously to the CPU cycle, the status of the clock memory can change several times during a long cycle.

5.4.9 Diagnostics buffer

The CPU supports a diagnostics buffer that contains an entry for each diagnostic event. Each entry includes a date and time the event occurred, an event category, and an event description. The entries are displayed in chronological order, with the most recent event at the top. When the log is full (500 events), a new event replaces the oldest event in the log. If the CPU loses power, the diagnostics buffer retains the 100 most recent diagnostic events.

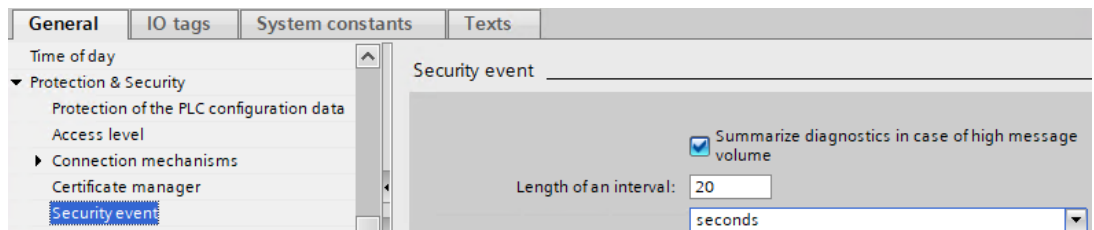
The following types of events are recorded in the diagnostics buffer:

- Each system diagnostic event; for example, CPU errors and module errors
- Each state change of the CPU (each power up, each transition to STOP, each transition to RUN)
- Each user diagnostic alarm generated by the Gen_UsrMsg instruction.

To access the diagnostics buffer, you must be online. From the "Online & diagnostics (Page 329)" view, locate the diagnostics buffer under "Diagnostics > Diagnostics buffer".

Reducing the number of security diagnostic events

Some security events generate repeated entries in the diagnostics buffer. These messages can fill up the diagnostics buffer and potentially obscure other event messages. You can configure the PLC to limit the number of diagnostic messages from security events. You make selections in the device configuration of the CPU based on the time interval in which you want to suppress recurring messages:



If you choose to summarize security events within a time interval, you have the choice of setting a time interval in seconds, minutes, or hours, and a numerical value in the range 1 .. 255.

If you choose to restrict security events, you will be restricting these types of events:

- Going online with the correct or incorrect password
- Manipulated communications data detected
- Manipulated data detected on memory card
- Manipulated firmware update file detected
- Changed protection level (access protection) downloaded to the CPU
- Password legitimization restricted or enabled (by instruction or CPU display)
- Online access denied due to the possible number of simultaneous access attempts being exceeded
- Timeout when an existing online connection is inactive
- Logging in to the Web server with the correct or incorrect password

5.4.10 Program alarms

The S7-1200 G2 allows you to create, edit, and monitor Program alarms in your STEP 7 project. These alarms deliver error messages or notifications about the PLC program running on your CPU.

From your STEP 7 project's Device configuration, select the "Diagnostics" tab and then select the "Alarm display" tab to view a log of Program alarms and their associated information. You can also configure Program alarms to display and be acknowledgeable in an HMI.

You can edit existing Program alarms in the Project tree under "PLC supervisions and alarms".

NOTE

The S7-1200 G2 CPU does not support supervisions.

See the following TIA Portal Information System topics for more detailed information on creating and editing Program alarms:

- Creating and editing alarms
(https://docs.tia.siemens.cloud/access?ft:originId=../4511680523/41028912907_enUS.htm&ft:clusterId./4511680523/41028912907.htm)
- Program Alarm: Generate program alarm with associated values
(https://docs.tia.siemens.cloud/access?ft:originId=../15889165323/41068416779_enUS.htm&ft:clusterId./15889165323/41068416779.htm)
- Program example for Get Alarm & Ack Alarms
(https://docs.tia.siemens.cloud/access?ft:originId=../15889165323/90334347915_enUS.htm&ft:clusterId./15889165323/90334347915.htm)

5.4.11 Time of day clock

The CPU supports a time-of-day clock. A super-capacitor supplies the energy required to keep the clock running during times when the CPU is powered down. The super-capacitor charges while the CPU has power. After the CPU has been powered up at least 24 hours, then the super-capacitor has sufficient charge to keep the clock running for typically 20 days.

STEP 7 sets the time-of-day clock to system time, which has a default value out of the box or following a factory reset. To utilize the time-of-day clock, you must set it. Timestamps such as those for diagnostics buffer entries, data log files, and data log entries, are based on the system time. You set the time of day from the "Set time of day" function (Page 329) in the "Online & diagnostics" view of the online CPU. STEP 7 then calculates the system time from the time you set plus or minus the Windows operating system offset from UTC (Coordinated Universal Time). Setting the time of day to the current local time produces a system time of UTC if your Windows operating system settings for time zone and daylight savings time correspond to your locale.

WARNING

Risk of attacker accessing your networks through open interfaces

If an attacker can access your networks through open interfaces, such as software like STEP 7, the SIMATIC Automation Tool, or through an HMI, the attacker can possibly disrupt control of your process by shifting the CPU system time.

The CPU supports "time of day" interrupts and clock instructions that depend upon accurate CPU system time. You must restrict access to the CPU by enabling access control and disabling the "Anonymous" user. Failure to do so can cause a security breach that allows an unknown user to disrupt control of your process by shifting the CPU system time.

Disruptions to process control can possibly cause death, severe injury, or property damage.

For security information and recommendations, see the "Operational Guidelines

(<https://www.siemens.com/global/en/products/services/cert/news/operational-guidelines-for-industrial-security.html>)" white paper on the Siemens Industrial Cybersecurity Website.

STEP 7 includes instructions (Page 180) to read and write the system time (RD_SYS_T and WR_SYS_T), to read the local time (RD_LOC_T), and to set the time zone (SET_TIMEZONE). The RD_LOC_T instruction calculates local time using the time zone and daylight saving time offsets that you set in the "Time of day" configuration in the general properties of the CPU (Page 166). These settings enable you to set your time zone for local time, optionally enable daylight saving time, and specify the start and end dates and times for daylight saving time. You can also use the SET_TIMEZONE instructions to configure these settings.

NOTE

Time zone differences

If you set the time of day clock and the time zone of your programming device is different from the time zone you configured in the device configuration for your CPU (Page 166), then you might see unexpected timestamps for items such as the following:

- Diagnostic buffer entries
- Data log files
- Entries in data logs

5.4.12 Data storage, memory areas, I/O and addressing

5.4.12.1 Accessing the data of the CPU

STEP 7 facilitates symbolic programming. You can create symbolic names or "tags" for I/O and memory. To use these tags in your user program, enter the tag name for the instruction parameter.

The CPU provides several options for storing data:

- **Global memory:** The CPU provides a variety of specialized memory areas, including inputs (I), outputs (Q) and memory (M). This memory is accessible by all code blocks without restriction.
- **PLC tag table:** You can enter symbolic names in the STEP 7 PLC tag table for specific memory locations. These tags are global to the STEP 7 program and allow programming with names that are meaningful for your application.
- **Data block (DB):** You can include DBs in your user program to store data for the code blocks. The data stored persists when the execution of the associated code block comes to an end. A "global" DB stores data that can be used by all code blocks, while an instance DB stores data for a specific FB and is structured by the parameters for the FB.
- **Temp memory:** Whenever the program calls a code block, the CPU allocates temporary, or local, memory (L) to be used during the execution of the block. When the execution of the code block finishes, the CPU reallocates the local memory for the execution of other code blocks.

Each memory location has a unique address. Your user program uses these addresses to access the information in the memory location. References to the input (I) or output (Q) memory areas, such as I0.3 or Q1.7, access the process image. To immediately access the physical input or output, append the reference with ":P" (such as I0.3:P, Q1.7:P, or "Stop:P").

You can force values [\(Page 339\)](#) for some memory areas. Some memory areas are retentive [\(Page 129\)](#) or optionally retentive.

Table 5-27 Memory areas

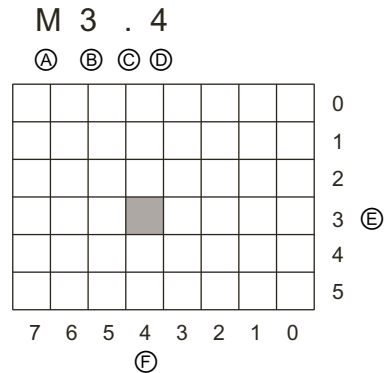
Memory area	Description	Force	Retentive
I Process image input I_:P ¹ (Physical input)	Copied from physical inputs at the beginning of the scan cycle	No	No
	Immediate read of the physical input points on the CPU, SB, and SM	Yes	No
Q Process image output Q_:P ¹ (Physical output)	Copied to physical outputs at the beginning of the scan cycle	No	No
	Immediate write to the physical output points on the CPU, SB, and SM	Yes	No
M Bit memory	Control and data memory	No	Yes (optional)
DB Data block	Data memory and also parameter memory for FBs	No	Yes (optional)
Temp memory	Temporary data for a block local to that block	No	No

¹ To immediately access (read or write) the physical inputs and physical outputs, append a ":P" to the address or tag (such as I0.3:P, Q1.7:P, or "Stop:P").

Each memory location has a unique address. Your user program uses these addresses to access the information in the memory location. The absolute address consists of the following elements:

- Memory area identifier (such as I, Q, or M)
- Size of the data to be accessed ("B" for Byte, "W" for Word, or "D" for DWord)
- Starting address of the data (such as byte 3 or word 3)

When accessing a bit in the address for a Boolean value, enter the memory area, the byte location, and the bit location for the data (such as I0.0, Q0.1, or M3.4).



A	Memory area identifier	E	Bytes of the memory area
B	Byte address: byte 3	F	Bits of the selected byte
C	Separator ("byte.bit")		
D	Bit location of the byte (bit 4 of 8)		

In the example, the memory area and byte address (M = bit memory area, and 3 = Byte 3) are followed by a period (".") to separate the bit address (bit 4).

5.4.12.2 Using absolute addressing to access CPU data

When using symbolic names for data ([Page 136](#)), you typically create tags either in the PLC tag table, a data block, or in the interface of an OB, FC, or FB. These tags include a name, data type, offset, and comment. Additionally, in a data block, you can specify a start value. You can use these tags when programming by entering the tag name at the instruction parameter.

Optionally, you can enter the absolute operand (memory area, size and offset) at the instruction parameter for most data types. The examples in the following sections show how to enter absolute operands. The % character is inserted automatically in front of the absolute operand by the program editor. You can toggle the view in the program editor to one of these: symbolic, symbolic and absolute, or absolute.

You cannot use absolute addressing for the long data types (64-bit) such as LWORD, LINT, ULINT, LREAL, LTIME, LTOD, and LDT. You must use symbolic addressing for the long data types.

I (process image input): The CPU samples the peripheral (physical) input points just prior to the cyclic OB execution of each scan cycle (Page 101) and writes these values to the input process image. You can access the input process image as bits, bytes, words, or double words. Both read and write access is permitted, but typically, process image inputs are only read.

Table 5-28 Absolute addressing for I memory

Bit	I[byte address].[bit address]	I0.1
Byte, Word, or Double Word	I[size][starting byte address]	IB4, IW5, or ID12

By appending a ":P" to the address, you can immediately read the digital and analog inputs of the CPU, SB, SM or distributed module. The difference between an access using I_:P instead of I is that the data comes directly from the points being accessed rather than from the input process image. This I_:P access is referred to as an "immediate read" access because the data is retrieved immediately from the source instead of from a copy that was made the last time the input process image was updated.

Because the physical input points receive their values directly from the field devices connected to these points, you cannot write to these points. I_:P accesses are read-only, as opposed to I accesses which can be read or written to.

I_:P accesses are also restricted to the size of inputs supported by a single CPU, SB, or SM, rounded up to the nearest byte.

For example, if the inputs of a 4 DI / 4 DQ SB are configured to start at I4.0, then the input points can be accessed as I4.0:P, I4.1:P, I4.2:P, and I4.3:P or as IB4:P. Accesses to I4.4:P through I4.7:P are not rejected, but make no sense since these points are not used. Accesses to IW4:P and ID4:P are prohibited since they exceed the byte offset associated with the SB.

Accesses using I_:P do not affect the corresponding value stored in the input process image.

Table 5-29 Absolute addressing for I memory (immediate)

Bit	I[byte address].[bit address]:P	I0.1:P
Byte, Word, or Double word	I[size][starting byte address]:P	IB4:P, IW5:P, or ID12:P

Q (process image output): The CPU copies the values stored in the output process image to the physical output points. You can access the output process image in bits, bytes, words, or double words. Both read and write access is permitted for process image outputs.

Table 5-30 Absolute addressing for Q memory

Bit	Q[byte address].[bit address]	Q1.1
Byte, Word, or Double word	Q[size][starting byte address]	QB5, QW10, QD40

By appending a ":P" to the address, you can immediately write to the physical digital and analog outputs of the CPU, SB, SM or distributed module. The difference between an access using Q_:P instead of Q is that the data goes directly to the points being accessed in addition to the output process image (writes to both places). This Q_:P access is sometimes referred to as an "immediate write" access because the data is sent immediately to the target point; the target point does not have to wait for the next update from the output process image.

Because the physical output points directly control field devices that are connected to these points, reading from these points is prohibited. That is, Q_:P accesses are write-only, as opposed to Q accesses which can be read or write.

Q_:P accesses are also restricted to the size of outputs supported by a single CPU, SB, or SM, rounded up to the nearest byte.

For example, if the outputs of a 4 DI / 4 DQ SB are configured to start at Q4.0, then the output points can be accessed as Q4.0:P, Q4.1:P, Q4.2:P, and Q4.3:P or as QB4:P. Accesses to Q4.4:P through Q4.7:P are not rejected, but make no sense since these points are not used. Accesses to QW4:P and QD4:P are prohibited since they exceed the byte offset associated with the SB.

Accesses using Q_:P affect both the physical output as well as the corresponding value stored in the output process image.

Table 5-31 Absolute addressing for Q memory (immediate)

Bit	Q[byte address].[bit address]:P	Q1.1:P
Byte, Word, or Double word	Q[size][starting byte address]:P	QB5:P, QW10:P or QD40:P

M (bit memory area): Use the bit memory area (M memory) for both control relays and data to store the intermediate status of an operation or other control information. You can access the bit memory area in bits, bytes, words, or double words. Both read and write access is permitted for M memory.

Table 5-32 Absolute addressing for M memory

Bit	M[byte address].[bit address]	M26.7
Byte, Word, or Double Word	M[size][starting byte address]	MB20, MW30, MD50

Temp (temporary memory): The CPU allocates the temp memory on an as-needed basis. The CPU allocates the temp memory for the code block and initializes the memory locations to 0 at the time when it starts the code block (for an OB) or calls the code block (for an FC or FB).

Temp memory is similar to M memory with one major exception: M memory has a "global" scope, and temp memory has a "local" scope:

- M memory: Any OB, FC, or FB can access the data in M memory, meaning that the data is available globally for all of the elements of the user program.
- Temp memory: The CPU restricts access to the data in temp memory to the OB, FC, or FB that created or declared the temp memory location. Temp memory locations remain local and different code blocks do not share temp memory, even when the code block calls another code block. For example: When an OB calls an FC, the FC cannot access the temp memory of the OB that called it.

The CPU limits memory as follows:

- 16 Kbytes temp (local) memory per block (OB/FB/FC)
- 64 Kbytes total temp (local) memory per event priority class.

You must consider each block's memory allocation and the nesting depth from the calling OB in planning memory usage.

You access temp memory by symbolic addressing only.

You can find out the amount of temp (local) memory that the blocks in your program use through the call structure in STEP 7. From the project tree select Program info and then select the Call structure tab. You will see all of the OBs in your program and you can drill down to see the blocks that they call. For each block, you can see the local data allocation. You can also access the Call structure display from the STEP 7 **Tools > Call structure** menu command.

DB (data block): Use the DB memory for storing various types of data, including intermediate status of an operation or other control information parameters for FBs, and data structures

required for many instructions such as timers and counters. You can access data block memory in bits, bytes, words, or double words. Both read and write access is permitted for read/write data blocks. Only read access is permitted for read-only data blocks.

Table 5-33 Absolute addressing for DB memory

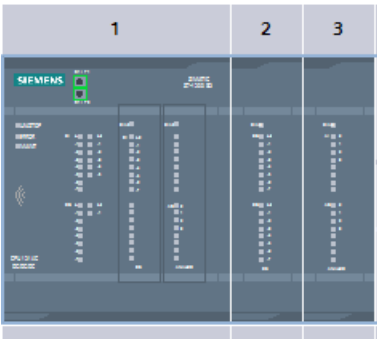
Bit	DB[data block number].DBX[byte address].[bit address]	DB1.DBX2.3
Byte, Word, or Double Word	DB[data block number].DB [size][starting byte address]	DB1.DBB4, DB10.DBW2, DB20.DBD8

NOTE

When you specify an absolute address in LAD or FBD, STEP 7 precedes this address with a "%" character to indicate that it is an absolute address. While programming, you can enter an absolute address either with or without the "%" character (for example %I0.0 or I.0). If omitted, STEP 7 supplies the "%" character.

In SCL, you must enter the "%" before the address to indicate that it is an absolute address. Without the "%", STEP 7 generates an undefined tag error at compile time

5.4.12.3 Addressing the local and expansion I/O



When you add a CPU and I/O boards or modules to your device configuration, STEP 7 automatically assigns input and output addresses. You can change the default addressing by selecting the address field in the device overview and entering new numbers.

- STEP 7 assigns digital inputs and outputs in groups of 8 points (1 byte), whether the module uses all the points or not.
- STEP 7 allocates analog inputs and outputs in groups of 4, where each analog point occupies 2 bytes.

The Device overview shows the I/O address assignments.

Device overview						
	Module	Slot	I address	Q address	Type	
		0				
	▼ G2_PL_C1_1	1			CPU 1214C DC/DC/DC	
	DI 14/DQ 10_1	1 8	0...1	0...1	DI 14/DQ 10	
	DI8 signal board (100 kHz)_1	1 9	4		DI8 signal board (100 kHz)	
	AQ4 Signal board 1	1 10		80...87	AQ4 Signal board	
	SM 1222 DQ16 x 24VDC_1	2		8...9	SM 1222 DQ16 x 24VDC	
	SM 1233 AI4/AQ4_1	3	112...119	112...119	SM 1233 AI4/AQ4	

This example represents the following configuration:

- CPU
- Signal board with 8 digital inputs
- Signal board with 4 analog outputs
- Signal module with 16 digital outputs
- Signal module with 4 analog inputs and 4 analog outputs

You can change I and Q addresses. STEP 7 assists you by preventing changes that are the wrong size or conflict with other addresses.

5.4.13 Processing of analog values

General purpose analog signal modules provide input signals or expect output values that represent either a voltage range or a current range. These ranges are as follows:

- Analog inputs: ± 10 V, ± 5 V, ± 2.5 V, 0 to 20 mA, or 4 to 20 mA
- Analog outputs: ± 10 V, 0 to 20 mA, or 4 to 20 mA

The values returned by the modules are integer values where 0 to 27648 represents the rated range for current, and -27648 to 27648 for voltage. Anything outside the range represents either an overflow or underflow. See the tables for analog input representation ([Page 442](#)) and analog output representation ([Page 443](#)) for details about the types of out-of-range values.

In your control program, you probably need to use these values in engineering units, for example to represent a volume, temperature, weight or other quantitative value. To do this for an analog input, you must first normalize the analog value to a real (floating point) value from 0.0 to 1.0. Then you must scale it to the minimum and maximum values of the engineering units that it represents. For values that are in engineering units that you need to convert to an analog output value, you first normalize the value in engineering units to a value between 0.0 and 1.0, and then scale it between 0 and 27648 or -27648 to 27648, depending on the range of the analog module. STEP 7 provides the NORM_X and SCALE_X instructions for this purpose. You can also use the CALCULATE instruction to scale the analog values.

Example: analog value processing

Consider, for example, an analog input that has a current range of 0 - 20 mA. The analog input module returns values in the range 0 to 27648 for measured values. For this example, consider that you are using this analog input value to measure a temperature range from 50 °C to 100 °C. A few sample values would have the following meanings:

Analog input value	Engineering units
0	50 °C
6192	62.5 °C
12384	75 °C
18576	87.5 °C
27648	100 °C

The calculation for determining engineering units from the analog input value in this example is as follows:

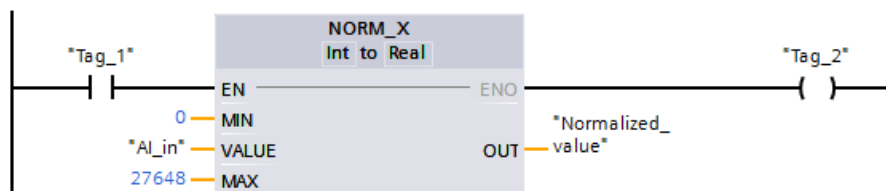
$$\text{Engineering units value} = 50 + (\text{Analog input value}) * (100 - 50) / (27648 - 0)$$

For the general case, the equation would be:

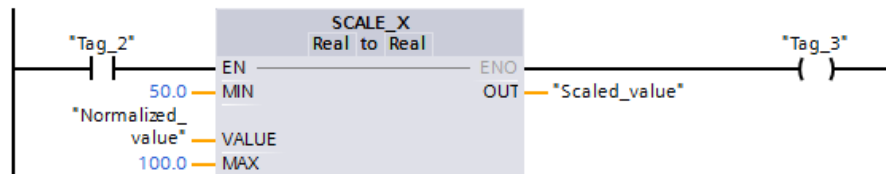
$$\begin{aligned} \text{Engineering units value} = & (\text{Low range of engineering units}) + \\ & (\text{Analog input value}) * \\ & (\text{High range of engineering units} - \text{Low range of engineering units}) / \\ & (\text{Maximum analog input range} - \text{Minimum analog input range}) \end{aligned}$$

In PLC applications, the typical method is to normalize the analog input value to a floating point value between 0.0 and 1.0. Then, you would scale the resulting value to a floating point value in the range of your engineering units. For simplicity, the following LAD instructions use constant values for the ranges; you might actually choose to use tags:

Network 1



Network 2



5.4.14 Using a memory card

5.4.14.1 Memory cards

NOTE

The CPU supports SIMATIC memory cards (Page 500) for the following purposes:

- Empty memory card (Page 145)
- Transfer card (Page 146)
- Program card (Page 148)
- Firmware update card (Page 152)
- Card for protection of confidential PLC configuration data (Page 154)

You can use supported non-SIMATIC memory cards (Page 500) only for transferring the license conditions and copyrights OSS information (Page 156) to a memory card.

Transfer cards and program cards contain the following elements if they exist in the project:

- Device configuration
- Code blocks
- Data blocks
- Technology objects
- Data logs
- Recipes
- User files

Transfer cards and program cards do not contain the following:

- Force tables
- Watch tables
- PLC tag tables

Use a transfer card to copy a program to the internal load memory (ILM) of the CPU without using STEP 7.

Use an empty transfer card to recover a password-protected CPU when you have lost or forgotten the password [\(Page 156\)](#).

Use a program card as external load memory for the CPU.

NOTE

Do not use the Windows formatter utility or any other formatting utility to reformat the memory card.

If a Siemens memory card is reformatted using the Microsoft Windows formatter utility, then the memory card will no longer be usable by any Siemens CPU.

Inability to use memory cards created with S7-1200 G2 V1.0

If you formatted a SIMATIC memory card for an S7-1200 G2 V1.0 CPU in the TIA Portal, the card is incorrectly formatted for use with firmware V4.1.

The invalid memory card prevents the CPU from starting. The Diagnostic buffer reports the error and the Status LEDs [\(Page 331\)](#) indicate the missing program memory card pattern.

To correct the card formatting problem, follow these steps:

1. Copy the memory card contents to your computer.*
2. Using the CPU that you upgraded to firmware V4.1, format the memory card from the TIA Portal.
3. Restore the memory card contents from your computer to the memory card.

*Do not include the system files crdinfo.bin and __LOG__.

5.4.14.2 Inserting a memory card in the CPU

NOTICE**Risks associated with electrostatic discharge**

Electrostatic discharge can damage the memory card or the receptacle on the CPU. If damaged, the receptacle or memory card can malfunction or become inoperable.

To protect the memory card and receptacle from electrostatic discharge, do the following:

- Make contact with a grounded conductive pad or wear a grounded wrist strap when handling the memory card.
- Store the memory card in a conductive container.

Receptacle or memory card malfunction can result in property damage.



Check that the memory card is not write-protected. Slide the protection switch away from the "Lock" position.

The memory card is keyed for proper installation. Insert the memory card with the correct orientation.

If you insert a write-protected memory card into the CPU, STEP 7 displays a diagnostic message on the next power up, alerting you to that fact. The CPU powers up without failure as long as the memory card you inserted is not blank. Instructions involving recipes or data logs, for example, return errors if the card is write-protected.

**WARNING****Verify that the CPU is not running a process before inserting the memory card.**

If you insert or remove a memory card of any type into a running CPU, the CPU restarts, resulting in diagnostic events, temporary loss of communication, and process disruption.

Before inserting or removing a memory card, always ensure that the CPU is not actively controlling a machine or process. Always install an emergency stop circuit for your application or process. Power off the CPU before inserting or removing a memory card.

Disruption of a running process can result in death, severe personal injury, and/or property damage.

NOTE

Do not insert program cards (Page 148) or transfer cards (Page 146) with S7-1200 projects into S7-1200 G2 CPUs.

S7-1200 projects are not compatible with version S7-1200 G2 CPUs. Inserting a memory card that is incompatible causes a CPU error.

If you do insert an invalid program card or transfer card, remove the card.

CPU behavior when you insert a memory card

When you insert a memory card in the CPU, the CPU restarts and performs the following steps:

1. Evaluates the card, and flashes the LEDs while evaluating
2. Performs actions based on the type of card:
 - Empty memory card (Page 145)
 - Transfer card (Page 146)
 - Program card (Page 148)
 - Firmware update card (Page 152)
 - Memory card for protecting confidential PLC configuration data (Page 154)
 - Memory card for copying license conditions and copyrights from the CPU (Page 156)

Procedure after card evaluation and processing

If the card is not an empty memory card (Page 145) or a program card (Page 148), power off the CPU and remove it.

After you remove the card, the CPU restarts and remains in STOP mode.

5.4.14.3 Empty memory card

An empty memory card does not have a job file (S7_JOB.S7S). The CPU behavior when you insert an empty memory card (Page 144) depends on the selection for "Disable copy from internal load memory to external load memory" in the "Protection & Security > External load memory" CPU properties (Page 166):

- If the check box is not selected, the CPU adds a job file. The CPU then copies internal load memory to external load memory (memory card) and erases internal load memory.
- If the check box is selected, the CPU does not create a program job file and it does not copy internal load memory to external load memory (memory card). It does not erase internal load memory.

If you insert a memory card that is not an empty memory card into the CPU, the configuration setting for "Disable copying from internal load memory to external load memory" has no effect on how the CPU evaluates the memory card.

5.4.14.4 Configuring the startup parameter of the CPU before copying the project to the memory card

When you copy a program to a transfer card or a program card, the program includes the startup parameter for the CPU (Page 166). Before copying the program to the memory card, always ensure that you have configured the operating mode for the CPU following a power-cycle. Select whether the CPU starts in STOP mode, RUN mode, or in the previous mode (prior to the power cycle).

5.4.14.5 Transfer card

NOTICE**Risks associated with electrostatic discharge**

Electrostatic discharge can damage the memory card or the receptacle on the CPU. If damaged, the receptacle or memory card can malfunction or become inoperable.

To protect the memory card and receptacle from electrostatic discharge, do the following:

- Make contact with a grounded conductive pad or wear a grounded wrist strap when handling the memory card.
- Store the memory card in a conductive container.

Receptacle or memory card malfunction can result in property damage.

Creating a transfer card

Configure the startup parameter of the CPU (Page 145) before copying a program to the transfer card.

To create a transfer card, follow these steps:

1. Insert an empty SIMATIC memory card that is not write-protected into an SD card reader/writer attached to your computer. (If the card is write-protected, slide the protection switch away from the "Lock" position.)

If you are reusing a SIMATIC memory card that contains a user program, data logs, recipes, or a firmware update, you **must** delete the files before reusing the card. Use Windows File Explorer to display the contents of the memory card and delete the following files and folders if they exist:

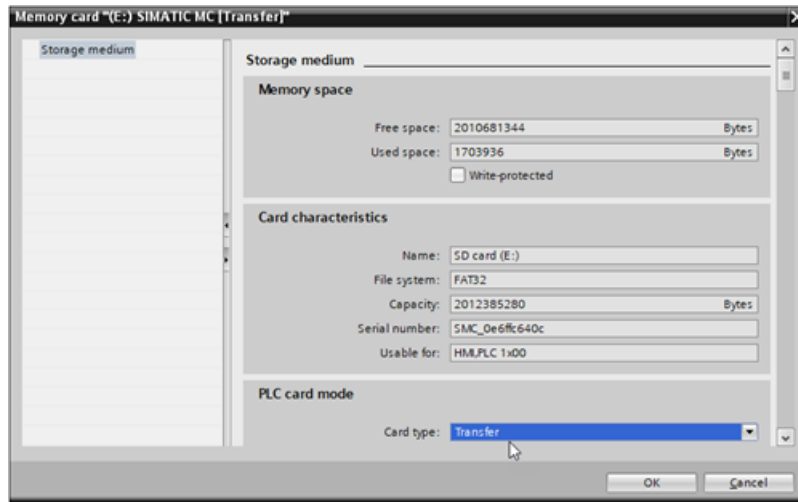
- S7_JOB.S7S
- SIMATIC.S7S
- FWUPDATE.S7S
- DataLogs
- Recipes
- UserFiles

NOTICE**Do NOT delete the hidden files "__LOG__" and "crdinfo.bin" from the memory card.**

The "__LOG__" and "crdinfo.bin" files are required for the memory card. If you delete these files, you cannot use the memory card with the CPU.

2. In the Project tree (Project view), expand the "Card Reader/USB memory" folder and select your card reader. If you are creating an empty transfer card, you can go to Step 6.
3. Add the program by selecting the CPU in the Project tree and dragging the CPU to the memory card. Another method is to copy the CPU and paste it to the memory card. Copying the CPU to the memory card opens the "Load preview" dialog.
4. In the "Load preview" dialog, click the "Load" button to copy the CPU to the memory card.

5. When the dialog displays a message that the CPU (program) has been loaded without errors, click the "Finish" button.
6. Right-click the drive letter corresponding to the memory card and select "Properties" from the shortcut menu.
7. In the "Memory card" dialog, select "Transfer" from the "Card type" drop-down menu and click OK.



8. Remove the transfer card from the card reader.

Using a transfer card

WARNING

Risks when inserting a transfer card

Inserting a memory card causes the CPU to restart and evaluate the card, which can affect the operation of an online process or machine.

Before inserting a transfer card, ensure that the CPU is in STOP mode and your process is in a safe state.

Unexpected operation of a process or machine can result in death or injury to personnel and/or property damage.

To transfer the program to a CPU, insert the transfer card into the CPU [\(Page 144\)](#). At this point, the existing program is still in the CPU.

The CPU evaluates the memory card and attempts to copy the program and all files on it to the internal load memory of the CPU. The CPU then responds as follows:

- If the copy process completes successfully, the MAINT LED flashes (yellow). Remove the transfer card.
- If the copy process fails for any reason, including exceeding the size of internal load memory (ILM), the copy aborts. The Diagnostic buffer shows an error. The ERROR LED blinks red and the STOP LED is solid yellow.

If the program transferred successfully, but data logs and recipes did not transfer, you can set the CPU to RUN mode after you remove the transfer card and the CPU restarts.

Instructions that require the missing data logs and recipes will report errors. You can retry the transfer if the failure occurred due to a disruption in the transfer process. If the failure was a result of ILM not having enough space for all the transfer card contents, you can delete some files from the transfer card and try again.

The CPU is in STOP mode after a transfer. The transfer card is unchanged.

See also

[Recovery from a lost password \(Page 156\)](#)

5.4.14.6 Program card

NOTICE

Risks associated with electrostatic discharge

Electrostatic discharge can damage the memory card or the receptacle on the CPU. If damaged, the receptacle or memory card can malfunction or become inoperable.

To protect the memory card and receptacle from electrostatic discharge, do the following:

- Make contact with a grounded conductive pad or wear a grounded wrist strap when handling the memory card.
- Store the memory card in a conductive container.

Receptacle or memory card malfunction can result in property damage.



Check that the memory card is not write-protected. Slide the protection switch away from the "Lock" position.

The memory card is keyed for proper installation. Insert the memory card with the correct orientation.

If you insert a write-protected memory card into the CPU, STEP 7 displays a diagnostic message on the next power up, alerting you to that fact. The CPU powers up without failure, but instructions involving recipes or data logs, for example, return errors if the card is write-protected.

Before you copy any program elements to the program card, delete any previously saved programs from the memory card.

Creating a program card

When used as a program card, the memory card is the external load memory of the CPU. If you remove the program card, the internal load memory of the CPU is empty. A program card includes the STEP 7 program and any data logs, recipes, or user files that belong to the program.

NOTE

If you insert an empty memory card into the CPU, the CPU copies the program and force values from internal memory to the memory card. After the copy has completed, the program in internal load memory is erased.

If you powered off the CPU before inserting the memory card, the CPU then goes to the configured startup mode (Page 145).

If you inserted the memory card without powering off, the CPU remains in STOP mode.

Always remember to configure the startup parameter of the CPU (Page 145) before copying a project to the program card. To create a program card, follow these steps:

1. Insert an empty SIMATIC memory card that is not write-protected into an SD card reader/writer attached to your computer.

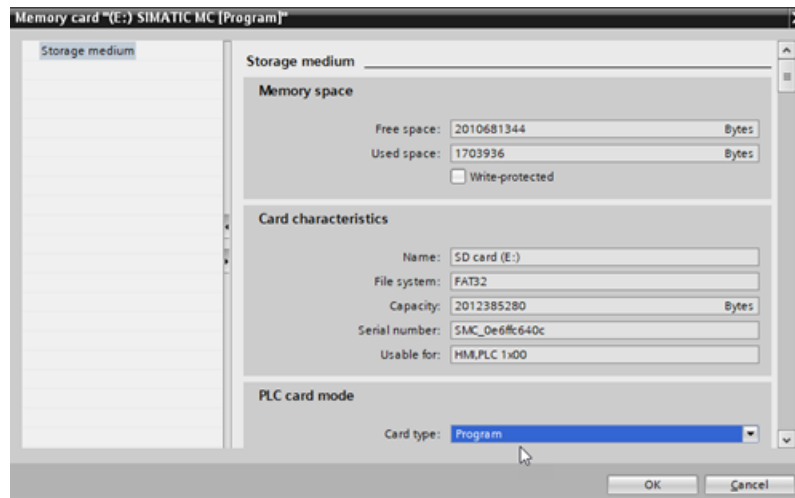
If you are reusing a SIMATIC memory card that contains a user program, data logs, recipes, or a firmware update, delete the files before reusing the card. Use Windows File Explorer to display the contents of the memory card and delete the following files and folders if they exist:

- S7_JOB.S7S
- SIMATIC.S7S
- FWUPDATE.S7S
- DataLogs
- Recipes
- UserFiles

NOTICE
Do NOT delete the hidden files "__LOG__" and "crdinfo.bin" from the memory card. The "__LOG__" and "crdinfo.bin" files are required for the memory card. If you delete these files, you cannot use the memory card with the CPU.

2. In the Project tree (Project view), expand the "Card Reader/USB memory" folder and select the card reader.
3. Display the "Memory card" dialog by right-clicking the drive letter corresponding to the memory card in the card reader and selecting "Properties" from the context menu.

4. In the "Memory card" dialog, select "Program" from the Card type dropdown menu.



5. Add the program by selecting the CPU device (such as G2_PLC_1 [CPU 1214C DC/DC/DC]) in the Project tree and dragging the CPU device to the memory card. (Another method is to copy the CPU device and paste it to the memory card.) Copying the CPU device to the memory card opens the "Load preview" dialog.
6. In the "Load preview" dialog, click the "Load" button to copy the CPU device to the memory card.
7. When the dialog displays a message that the download completed without errors, click the "Finish" button.

Using a program card as the load memory for a CPU

WARNING

Risks associated with inserting a program card

Use caution when inserting a program card while the CPU is in RUN mode. If you insert a program card into a CPU, the CPU restarts. Unexpected equipment operation can occur.

Ensure that the CPU is in STOP mode before inserting a program card.

Unexpected equipment operation can result in death, injury, and equipment damage.

To use a program card with a CPU, insert the program card (Page 144) into the CPU. The CPU evaluates the program card and erases the internal load memory of the CPU.

The program card must then remain in the CPU.

 WARNING

Risks associated with removing a program card

If a program card is removed while the CPU is in RUN mode, the CPU restarts.

Use caution when removing a program card while the CPU is in RUN mode. Removing the program card removes the program from the CPU.

Unexpected equipment operation can occur resulting in death, injury, and equipment damage.

Service life of a SIMATIC memory card

The service life of a SIMATIC memory card depends on factors such as the following:

- Number of delete and write operations per memory block
- Number of bytes written
- External influences, such as ambient temperature

NOTE

Effect of write and delete operations on SIMATIC memory card service life

Write or delete operations, particularly repeated (cyclic) write/delete operations, reduce the service life of the SIMATIC memory card.

Cyclic execution of the following actions reduces the service life of the memory card depending on the number of write operations and data:

- Data Log handling (for example, DataLogWrite)
 - Recipe handling (for example, RecipeExport)
 - System Function Calls (SFCs) that write/delete to the file system (for example, WRIT_DBL, CREATE)
 - System Function Blocks (SFBs) that write/delete to file system (for example, FileWriteC, FileDelete)
 - Any other cyclic action that changes data on the persistent store (for example, Tracing, SET-TimeZone)
-

5.4.14.7 Firmware update card

You can use a SIMATIC memory card for performing a firmware update.

NOTE

You cannot update an S7-1200 CPU to S7-1200 G2 by firmware update.

Firmware updates are available on the Siemens Industry Online Support (<https://sieportal.siemens.com/en-ww/support>) Web site. From this Web site, navigate to "Downloads". From there, search for the specific type of module that you need to update.

Alternatively, you can access the downloads Web page (<https://support.industry.siemens.com/cs/ww/en/ps/13639/dl>) directly. Filter the downloads for S7-1200 G2 or a specific article number.

NOTICE**Risks associated with electrostatic discharge**

Electrostatic discharge can damage the memory card or the receptacle on the CPU. If damaged, the receptacle or memory card can malfunction or become inoperable.

To protect the memory card and receptacle from electrostatic discharge, do the following:

- Make contact with a grounded conductive pad or wear a grounded wrist strap when handling the memory card.
- Store the memory card in a conductive container.

Receptacle or memory card malfunction can result in property damage.

You can also use one of these methods to perform a firmware update:

- Online and diagnostic tools of STEP 7 ([Page 329](#))
- SIMATIC Automation Tool (<https://support.industry.siemens.com/cs/ww/en/view/98161300>)

Downloading and installing a firmware update

To download the firmware update to your memory card, follow these steps:

1. Insert an empty SIMATIC memory card that is not write-protected into an SD card reader/writer attached to your computer. If the card is write-protected, slide the protection switch away from the "Lock" position.

You can reuse a SIMATIC memory card that contains a user program or another firmware update. To avoid any confusion, you should also delete files S7_JOB.S7S, SIMATIC.S7S, and FWUPDATE.S7S if they exist.

NOTE

Do NOT delete the hidden files "__LOG__" and "crdinfo.bin" from the memory card.

The "__LOG__" and "crdinfo.bin" files are required for the memory card. If you delete these files, you cannot use the memory card with the CPU.

2. Select the zip file for the firmware update that corresponds to your module, and download it to your computer. Double-click the file, set the file destination path to be the root directory of the SIMATIC memory card, and start the extraction process. After the extraction is complete, the root directory (folder) of the memory card will contain a "FWUPDATE.S7S" directory and the "S7_JOB.S7S" file.

NOTE

Do not put multiple firmware updates for the same article number (MLFB) on your memory card. Putting multiple updates for the same article number on the memory card causes the firmware update to fail.

You can put multiple firmware updates for different article (MLFB) numbers on a single memory card. This allows you to use a single memory card to update the firmware of multiple station hardware modules.

3. Safely eject the card from the card reader/writer.

Installing a firmware update

** WARNING****Risks when installing firmware updates**

Installing the firmware update causes the CPU to restart, which can affect the operation of an online process or machine.

Verify that the CPU is not actively running a process before installing the firmware update. Before inserting the memory card, always ensure that the CPU is offline and in a safe state.

Unexpected operation of a process or machine can result in death or injury to personnel and/or property damage.

To install the firmware update, insert the firmware update card into the CPU ([Page 144](#)).

After you insert the card, the firmware update starts. When the MAINT LED flashes (yellow), the firmware update has finished. Remove the firmware update card. A firmware update does not affect the STEP 7 program and device configuration.

During update, the firmware update procedure ignores UPD files that do not correspond to any station hardware modules. If you have multiple station hardware modules with the same article number (MLFB), the firmware update is installed on all of those modules. This allows you to create a master firmware update memory card to update all stations in your facility.

If you powered off the CPU before removing the memory card, the CPU then goes to the configured startup mode ([Page 145](#)).

If you removed the memory card without powering off, the CPU remains in STOP mode.

The Diagnostics buffer includes entries when firmware update attempts are made, whether successful or not. In the case of a failure, the Diagnostics buffer message provides an explanation for the failure. You can then easily scan the Diagnostics buffer for any unexpected anomalies.

5.4.14.8 Memory card for protecting confidential PLC configuration data

You can use a SIMATIC memory card to set or remove the password for Protection of confidential PLC configuration data. To change an existing password for Protection of confidential PLC configuration data, you must first clear the existing password and then set the new password.

NOTICE**Risks associated with electrostatic discharge**

Electrostatic discharge can damage the memory card or the receptacle on the CPU. If damaged, the receptacle or memory card can malfunction or become inoperable.

To protect the memory card and receptacle from electrostatic discharge, do the following:

- Make contact with a grounded conductive pad or wear a grounded wrist strap when handling the memory card.
- Store the memory card in a conductive container.

Receptacle or memory card malfunction can result in property damage.

Risks associated with the decommissioning process

S7-1200 G2 CPUs do not support secure erasure of the memory card and internal flash. Therefore, during the decommissioning process, you must securely dispose of the CPU and memory card to prevent the loss of proprietary or confidential information.

How to create a memory card with a Protection of confidential PLC configuration data password

To create the memory card with this password, follow these steps:

1. Insert an empty SIMATIC memory card that is not write-protected into an SD card reader/writer attached to your computer. If the card is write-protected, slide the protection switch away from the "Lock" position.
You can reuse a SIMATIC memory card that contains a user program or firmware update, but you must delete some of the files on the memory card. To reuse a memory card, you must delete the "S7_JOB.S7S" file before creating the Protection of confidential PLC configuration data file. Use Windows Explorer to display the contents of the memory card and to delete the "S7_JOB.S7S" file.

NOTICE**Do NOT delete the hidden files "__LOG__" and "crdinfo.bin" from the memory card.**

The "__LOG__" and "crdinfo.bin" files are required for the memory card. If you delete these files, you cannot use the memory card with the CPU.

2. Create a file on the root of the memory card called "S7_JOB.S7S". Open the file with a text editor and type the following: SET_PWD.
3. Create a folder on the root of the memory card called: SET_PWD.S7S.
4. Under the "SET_PWD.S7S" folder, create a text file called "PWD.TXT". The file must be named "PWD.TXT".

5. Enter your Protection of confidential PLC configuration data password as the text contents of the file. The file must contain a single line of text representing the Protection of confidential PLC configuration data password. Follow the STEP 7 rules for passwords when creating the password, using these characters:
 - 0123456789
 - A...Z a...z
 - !#\$%&()*+,-./:;<=>?@ [_{}~^
6. Safely eject the card from the card reader/writer.

How to use a memory card to clear the Protection of confidential PLC configuration data password

To clear the Protection of confidential PLC configuration data password, follow these steps to create a memory card with an empty password, and then use that card to clear the password in the CPU:

1. Follow steps 1 - 4 above to create a memory card with the required structure.
2. Leave the PWD.TXT file empty.
3. Insert the memory card (Page 144) with no password into the CPU. The CPU evaluates the card and clears the Protection of confidential PLC configuration data password.
4. Remove the memory card. After the CPU restarts, it has no Protection of confidential PLC configuration data password.

How to set the Protection of confidential PLC configuration data password

To set the Protection of confidential PLC configuration data password, follow these steps:

1. Verify that the CPU is not actively running a process before setting the Protection of confidential PLC configuration data password.
2. Insert the memory card (Page 144) you created with your password into the CPU. The CPU evaluates the card and sets the Protection of confidential PLC configuration data password.
3. Remove the memory card. After the CPU restarts, it uses the new Protection of confidential PLC configuration data password.

If the existing program requires the Protection of confidential PLC configuration data password you set with the memory card, the PLC can go to RUN based on the project configuration.

If the existing user program requires a different Protection of confidential PLC configuration data password than what you set with the memory card, the program will not load after restarting. You must clear the existing program and download a program that uses the Protection of confidential PLC configuration data password that you set in the previous steps.

5.4.14.9 Recovery from a lost password

If you have lost the password for a password-protected CPU, use an empty transfer card (Page 146) to delete the password-protected program. The empty transfer card erases the internal load memory of the CPU. You can then download a new user program from STEP 7 to the CPU.

WARNING

Risks when inserting transfer cards

If you insert a transfer card in a running CPU, the CPU goes to STOP. Control devices can fail in an unsafe condition, resulting in unexpected operation of controlled equipment.

Verify that the CPU is not actively running a process before inserting the memory card. Before inserting a transfer card, always ensure that the CPU is in STOP mode and your process is in a safe state.

Such unexpected operations can result in death or serious injury to personnel, and/or damage to equipment

You must remove the transfer card before setting the CPU to RUN mode.

5.4.14.10 Memory card for copying license conditions and copyrights from the CPU

License conditions and copyright files for open-source and third-party software (OSS files) are embedded in the CPU firmware. You can copy them to a supported non-SIMATIC standard memory card (Page 500).

Copying license conditions and copyrights to a non-SIMATIC memory card

To copy the license conditions and copyright files to a supported non-SIMATIC standard memory card, insert a supported non-SIMATIC standard memory card (Page 144) into the CPU. The format of the memory card must be "FAT32" file system.

The CPU restarts and copies the license conditions and copyrights to the memory card. They are in a zip file in a folder named OSS at the root level of the memory card file system. You can remove the memory card.

5.4.14.11 Using a memory card with the S7-1200 G2 fail-safe CPU

The S7-1200 G2 fail-safe CPU behavior when using a memory card has some differences from the standard CPU:

- When the S7-1200 G2 fail-safe CPU starts with no memory card and the Internal Load Memory (ILM) is empty, the fail-safe CPU's STOP and MAINT LEDs flash for three seconds. Power cycle the CPU. This provides a temporary visual indication that the ILM is empty. You must use the TIA Portal, the SIMATIC Automation Tool, or a memory card to load a user program.
- When the fail-safe CPU starts with a program memory card installed and the ILM is not empty, the fail-safe CPU erases the ILM, flashes the STOP and MAINT LEDs, and waits for user action. This is a visual indication that the ILM is erased and that the fail-safe CPU is waiting for a power cycle or a memory reset command in order to continue. After the power cycle or memory reset, subsequent power cycles load the program from the memory card.
- When the fail-safe CPU starts with an empty memory card installed and the ILM is not empty, the fail-safe CPU copies the program from the ILM to the memory card. The fail-safe CPU then erases the ILM, flashing the STOP and MAINT LEDs, and waits for user action. This is an indication that the ILM is erased and that the fail-safe CPU is waiting for a power cycle or a memory reset command in order to continue. After the power cycle or memory reset, subsequent power cycles load the program from the memory card.
- When the fail-safe CPU starts with a transfer memory card installed and the ILM is not empty, the fail-safe CPU erases the ILM, flashing the STOP and MAINT LEDs. This is a visual indication that the ILM is erased and that the fail-safe CPU is waiting for a power cycle or a memory reset command in order to continue. After the power cycle or memory reset, the fail-safe CPU copies the user program from the memory card to the ILM, and the fail-safe CPU stops, with the STOP LED on and the MAINT LED flashing. At this point, you must remove the transfer memory card. After the fail-safe CPU restarts, subsequent power cycles load the program from the ILM.

Refer to the "SIMATIC Safety - Configuring and Programming, Programming and Operating Manual", "Function test of safety program and protection through program identification" for instructions on transferring programs.

WARNING

Loading an incorrect user program into a fail-safe CPU results in incorrect execution and total or partial loss of the safety function.

Loss of the safety function can result in unexpected machine or process operation, which can cause death, severe personal injury, and/or property damage.

Follow the instructions as provided in the *SIMATIC Safety - Configuring and Programming, Programming and Operating Manual* for properly identifying safety programs and controlling how you load programs into a fail-safe CPU.

See also

SIMATIC Safety - Configuring and Programming manual
(<https://support.industry.siemens.com/cs/us/en/view/54110126>)

5.5 Managing users and roles

With the TIA Portal you can perform user management and access control (UMAC). This allows you to create and manage users and roles in your project who are allowed to perform specific functions. You can assign roles with specific rights to each user. You can then assign runtime rights to your S7-1200 G2 PLC.

You can also create and manage central users outside the TIA Portal in UMC (User Management Component). UMC provides the capability to define users and roles in a central location that can then be used across multiple projects.

After adding users and making role assignments, you must load the project to the CPU(s) to activate UMAC. After you load the project to your S7-1200 G2 PLC, only authorized users can access various CPU functions (Page 329).

For more information, refer to "Managing users and roles" in the TIA Portal Information System.

5.6 Device configuration

5.6.1 Overview

You create the device configuration for your PLC by adding a CPU and additional boards and modules to your project as needed.

0	1	2	3	4	5	6

① PROFINET port(s) of CPU (under door)

② Signal board (SB) or Communication board (CB)

③ CPU

④ Communication module (CM) or Communication processor (CP)

⑤ Signal module (SM) for digital or analog I/O

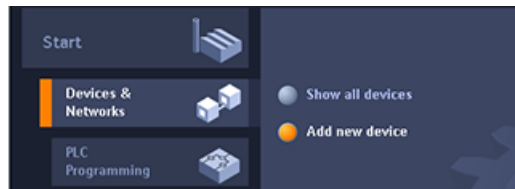
To learn more about the number of modules you can configure in your project, see [Installing and removing expansion modules \(Page 74\)](#).

Refer to [Ordering Information \(Page 498\)](#) for expansion boards and modules that are available.

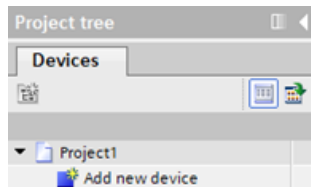
5.6.2 Inserting a CPU

You can insert a CPU into your project from either the Portal view or the Project view of STEP 7:

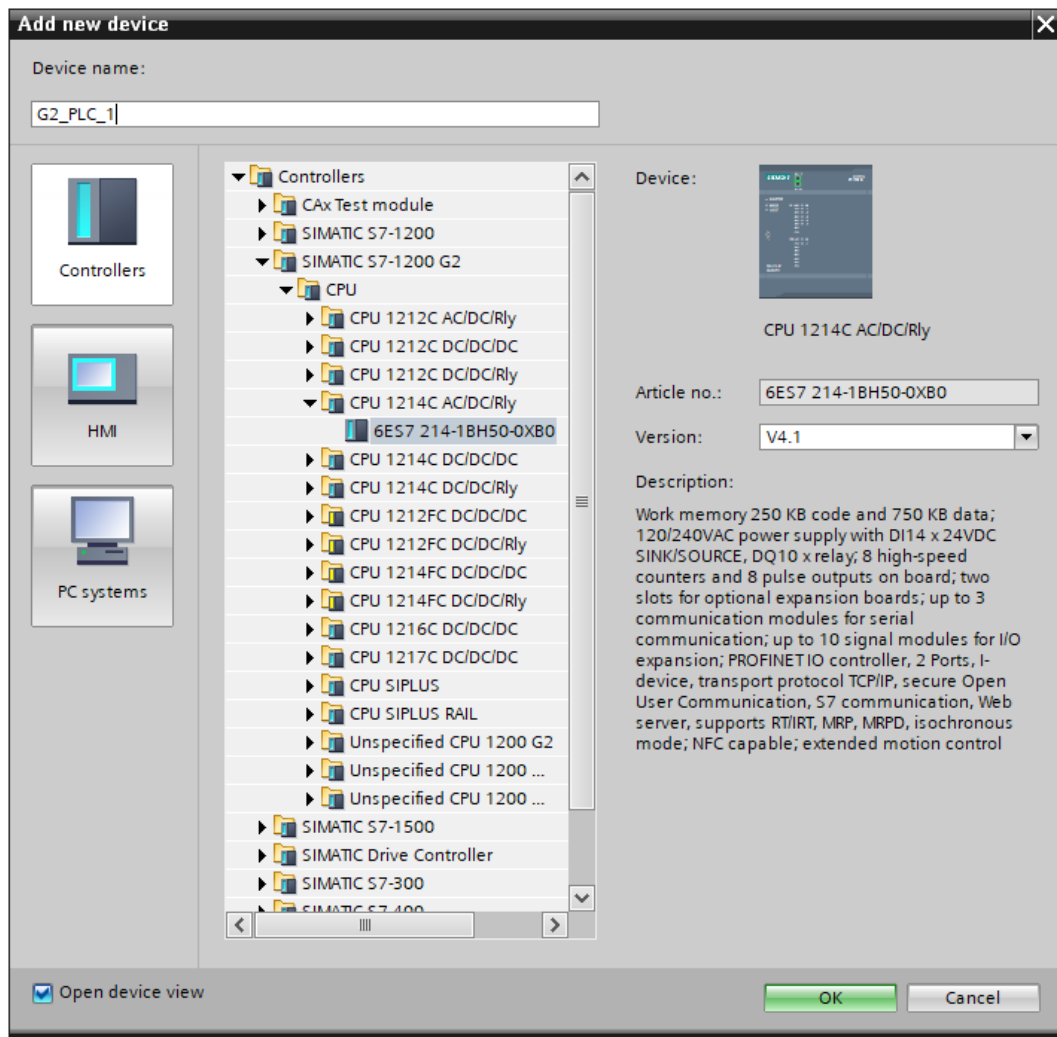
- In the Portal view, select "Devices & Networks" and click "Add new device".



- In the Project view, under the project name, double-click "Add new device".



From the "Add new device" dialog, select the correct Article Number and firmware version from the list.

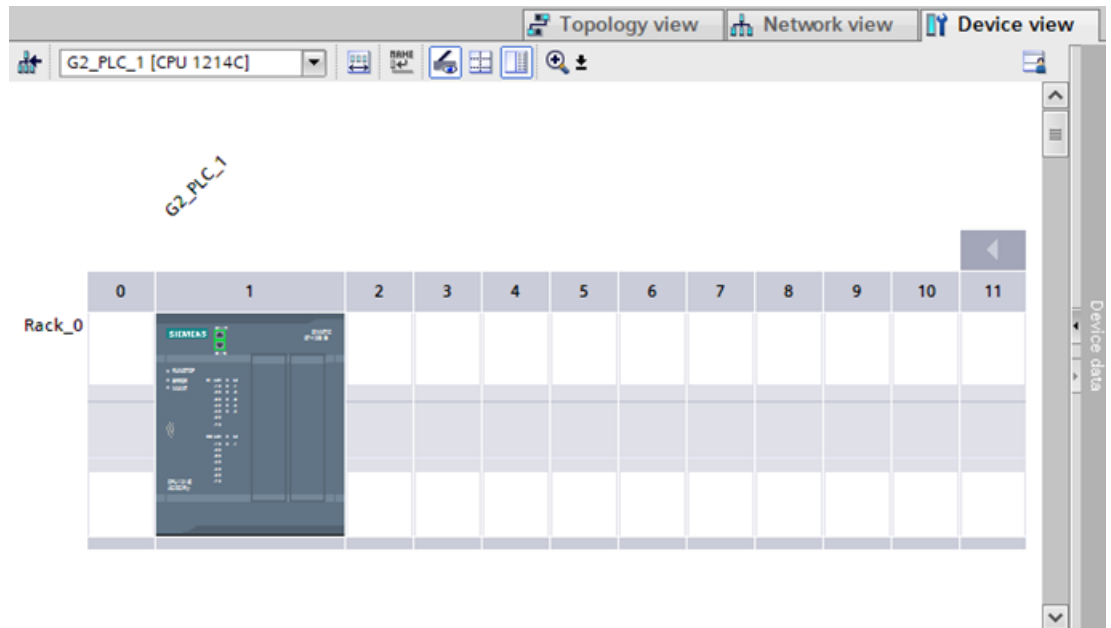


Configuring PLC security settings for your inserted CPU

When you insert an S7-1200 G2 CPU, STEP 7 launches the security wizard to help you set up your PLC security settings. Follow the steps in the wizard to set up your PLC security settings. Refer to Protection & Security topics in the TIA Portal Information System to learn more about each configuration task and related security concepts.

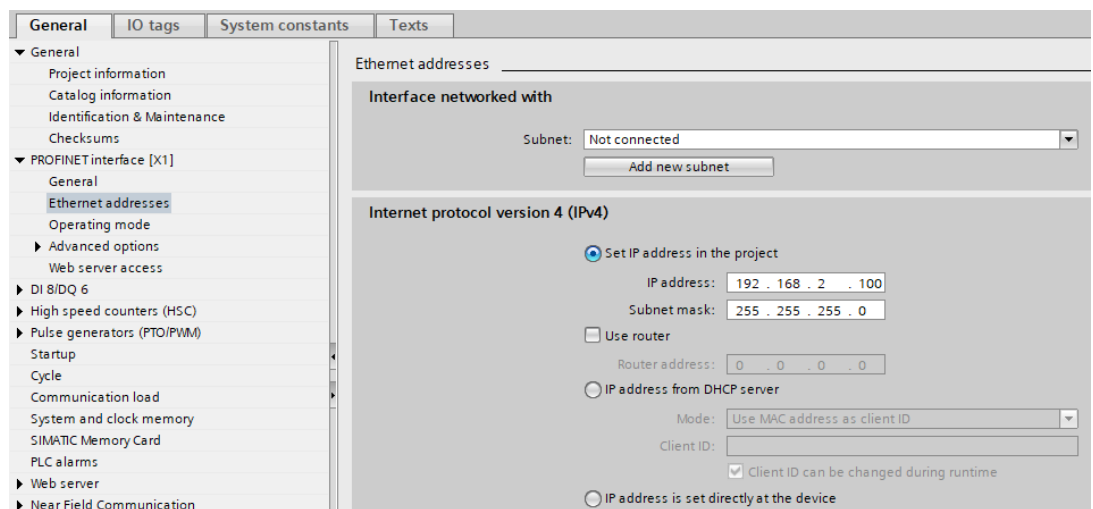
Device configuration for the inserted CPU

After you add a CPU, STEP 7 creates the rack and displays the CPU in the Device view:



Clicking the CPU in the Device view displays the CPU properties in the inspector window.

You can assign an IP address for the CPU during the device configuration. If your CPU is connected to a router on the network, select the checkbox next to "Use router" and enter the router's IP address.



5.6.3 Uploading the configuration of a connected CPU

STEP 7 provides two methods for uploading the hardware configuration of a connected CPU:

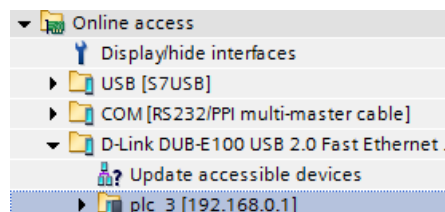
- Uploading the connected device as a new station
- Configuring an unspecified CPU and detecting the hardware configuration of the connected CPU

Note that the first method uploads both the hardware configuration and the software of the connected CPU.

Uploading a device as a new station

To upload a connected device as a new station, follow these steps:

1. Expand your communications interface from the "Online access" node of the project tree.



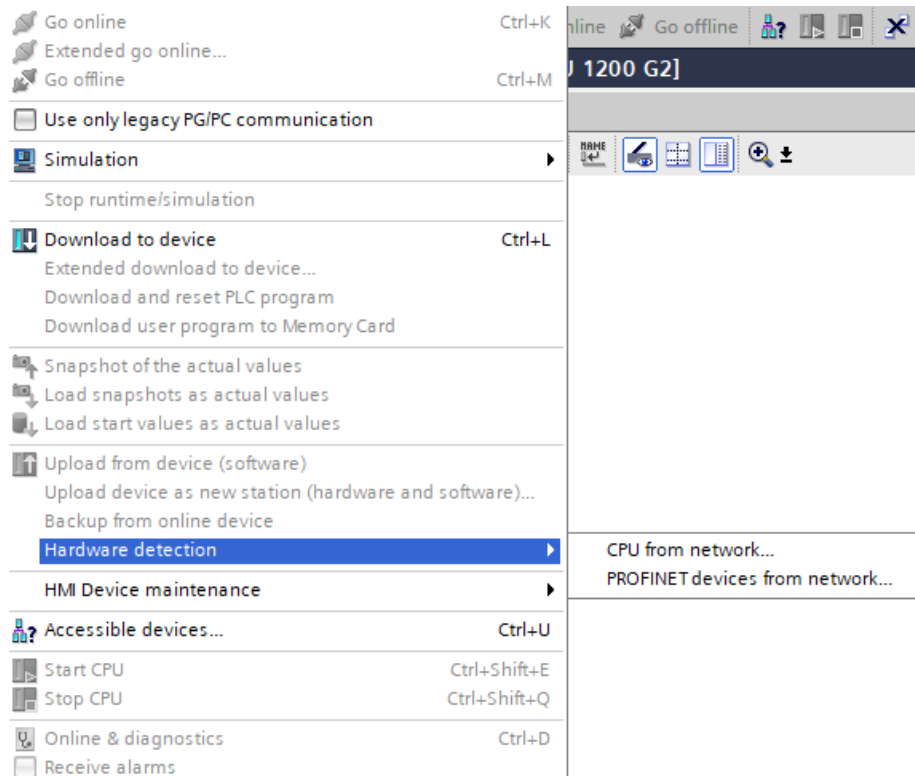
2. Double-click "Update accessible devices".
3. Select the PLC from the detected devices.
4. From the Online menu of STEP 7, select the "Upload device as new station (hardware and software)" menu command.

STEP 7 uploads both the hardware configuration and the program blocks.

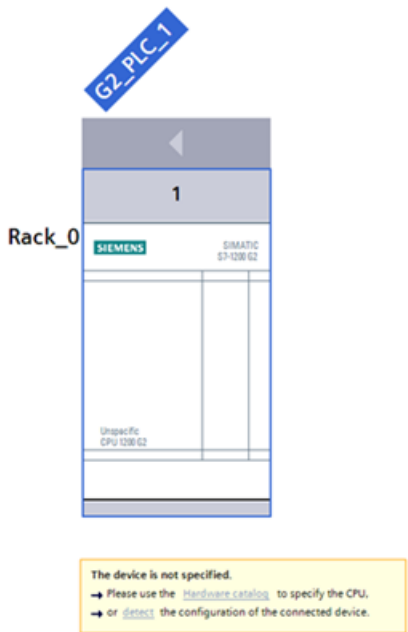
Detecting the hardware configuration of an unspecified CPU

If you are connected to a CPU, you can upload the configuration of that CPU, including any modules, to your project. Create a new project and use "Add new device ([Page 165](#))" to add an "Unspecific S7-1200 G2 CPU".

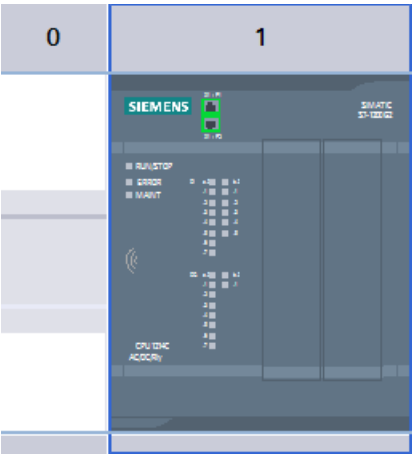
From the program editor, select the "Hardware detection" command from the "Online" menu.



From the device configuration, select "detect" in the box below the CPU. STEP 7 then detects the configuration of the PLC.



After you select the CPU from the online dialog and click Load, STEP 7 uploads the hardware configuration from the CPU, including any devices. You can then configure the parameters for the CPU and the modules (Page 166).



NOTE

Increased CPU Power-on time with missing/unplugged modules

Powering the CPU while it has missing or unplugged modules relative to your downloaded configuration causes an increased power-on time. During this period, the CPU and NFC functionality (Page 315) are unresponsive due to a longer CPU startup time. The length of the timeout for SBs is shorter than for CMs or SMs.

5.6.4 Adding modules to the configuration

Use the STEP 7 hardware catalog to add any of the following expansion modules or expansion boards to the CPU device configuration:

- Signal modules (SM) provide additional digital or analog I/O points. These modules are connected to the right side of a CPU, CM, CP, or SM.
- Signal boards (SB) provide additional I/O points for the CPU. The SB is installed on the front of the CPU.
- A Communication board (CB) provides an additional communication port (such as RS485). The CB is installed on the front of the CPU.
- A Communication module (CM) or Communication processor (CP) provides an additional communication port (such as RS232/RS485/RS422). Either module is connected to the right side of a CPU, CM, or CP.
- A Battery board (BB) provides long-term backup for the CPU's Real-Time Clock (RTC). The BB is installed in an SB slot on the front of the CPU. You can only add one BB to the device configuration.

To learn more about possible configurations of expansion modules, see [S7-1200 G2 Modules \(Page 59\)](#).

To insert a module into the device configuration, select the device in the hardware catalog and either double-click or drag the device to the appropriate slot. If you have one or more CMs or CPs in your project, add them to the right of the CPU before adding any SMs. An invalid module order causes a compile error. You must download your device configuration to the CPU for the devices to be functional.

5.6.5 Configuring the operation of the CPU

STEP 7 enables you to configure your S7-1200 G2 CPU by editing the CPU properties listed below. You can change Startup behavior, modify the behavior of digital I/O, or enable security settings, in addition to other valuable functions.

To configure the operational parameters for the CPU, select the CPU in the Device view and use the "Properties" tab of the inspector window.

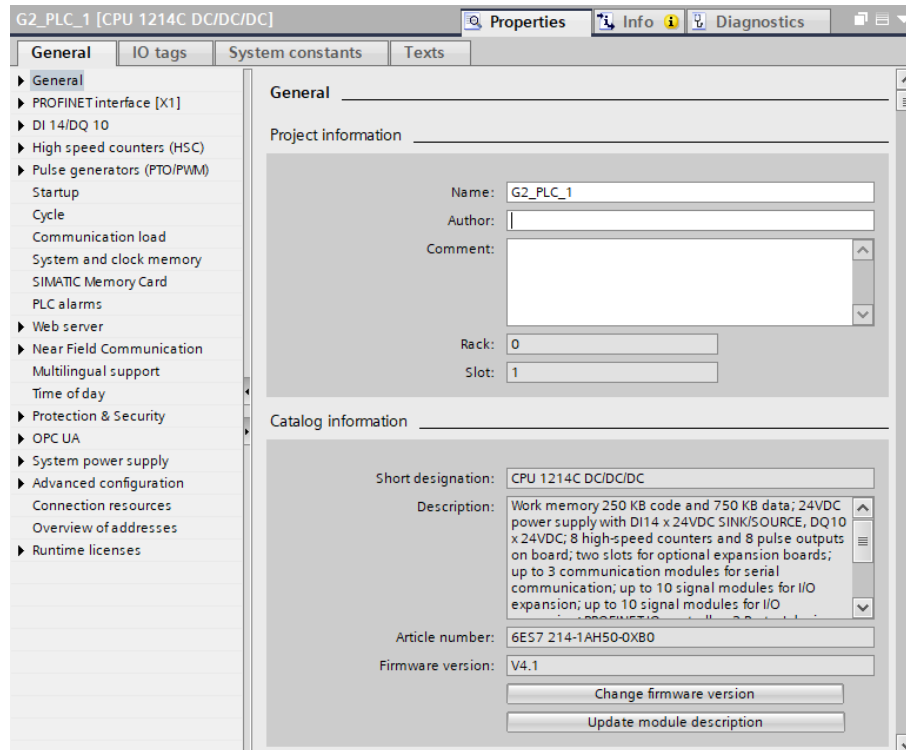


Table 5-34 CPU properties

Property	Description
General	Contains Project information, Catalog information, Identification & Maintenance, and Checksums.
PROFINET interface	Sets the IP address and Advanced PROFINET features.
DI and DQ	Configures the behavior of the local (onboard) digital I/O (for example, digital input filter times and digital output reaction to a CPU stop).
High-speed counters (Page 182) and pulse generators (Page 180)	Enables and configures the high-speed counters (HSC) and the pulse generators used for pulse train output (PTO) and pulse-width modulation (PWM). When you configure a digital output of the CPU or signal board (SB) as an HSC Compare output, or as a pulse output for use with PWM, PTO, or motion control instructions, that physical output is now controlled by the HSC or pulse-generator function. The corresponding process-image value is no longer written to that physical output; changes to the process image will be ignored by a physical output assigned to an HSC or pulse generator.

¹ If you disable access control, every user has full access to the CPU without a password. You are essentially granting users "Full access (no protection)" (if using a standard CPU) or "Full access incl. fail-safe (no protection)" (if using an F-CPU). Users can access most CPU functions. Because of this, Siemens recommends disabling access control only during commissioning and that only authorized persons have access to the CPU during this phase.

Property	Description
Startup (Page 103)	Startup after POWER ON: Selects the behavior of the CPU following an off-to-on transition, such as to start in STOP mode or to go to RUN mode after a warm restart. Comparison preset to actual configuration: Specifies the startup characteristics of the CPU for situations in which the actual configuration of the S7-1200 G2 station does not correspond to the preset configuration: - Startup of the CPU only if compatible - Startup of the CPU even if mismatch A module in the configured slot must be compatible with the configured module. Compatible means that the module that is present matches the number of inputs and outputs and must match with respect to its electrical and functional properties. It may be more capable, but not less capable. Beginning with S7-1200 G2 firmware version V4.1, this setting applies to configurations with missing SMs, SBs, CMs, CPs, or CBs. Configuration time: Specifies a maximum amount of time (default: 60000 ms) in which the local I/O and distributed I/O must start up. (The CMs receive power and communication parameters from the CPU during startup. This assignment time allows time for the I/O connected to the CM to be brought online.) The CPU goes to RUN as soon as the local I/O and distributed I/O have started and are ready for operation, regardless of the assignment time. If the local I/O and distributed I/O have not been brought online within this time, the CPU still goes to RUN--without the local I/O and distributed I/O.
Cycle (Page 126)	Defines a maximum cycle time or a fixed minimum cycle time.
Communication load	Allocates a percentage of the CPU time to be dedicated to communication tasks.
System and clock memory (Page 131)	Enables a byte for "system memory" functions and enables a byte for "clock memory" functions (where each bit toggles on and off at a predefined frequency).
SIMATIC Memory Card	Allows you to configure the CPU to determine when the SD card has aged to a configured percentage value. You can select the "Aging of the SIMATIC Memory card" checkbox to configure the threshold value percentage. You can use the GetSMCInfo instruction to check the SIMATIC memory card against this configured value.
PLC alarms	Enables central alarm management, allowing the CPU to transfer alarm text to the HMI device.
Web server (Page 316)	Enables and configures the Web server feature.
Near Field Communication (Page 315)	Enables reading data from a supported CPU with the S7-1200 G2 NFC app.
Multilingual support	Assigns a project language for the device and the Web server to use for displaying diagnostics buffer entry texts for each of the possible Web server user interface display languages.
Time of day	Selects the time zone and configures daylight saving time. Allows for Time Synchronization across plant components.

¹ If you disable access control, every user has full access to the CPU without a password. You are essentially granting users "Full access (no protection)" (if using a standard CPU) or "Full access incl. fail-safe (no protection)" (if using an F-CPU). Users can access most CPU functions. Because of this, Siemens recommends disabling access control only during commissioning and that only authorized persons have access to the CPU during this phase.

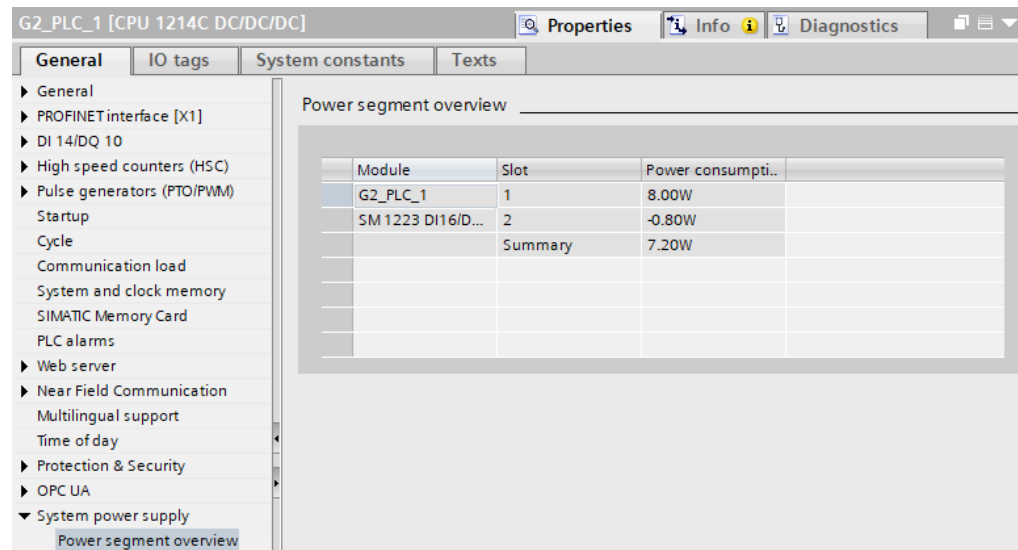
Property	Description
Protection & Security	Protection of the PLC configuration data https://docs.tia.siemens.cloud/access?ft:originId=/10866368523/141646478219_enUS.htm&ft:clusterId=/10866368523/141646478219.htm: Allows for password protection of confidential PLC configuration data. Access control: Allows for disabling or enabling access control and, optionally, access levels.¹ Lockout of user account at runtime: Allows for the configuration of settings for the lockout of user accounts following a failed login attempt. Connection mechanisms (Page 220): Permits access with PUT/GET communication from a remote partner when the Anonymous user is enabled. Allows for configuration of secure PG/HMI certificate-based communication. Certificate manager (Page 220): Enables certificate-based security settings for global or partner devices. Syslog: Allows for the logging and non-retentive storage of critical operations event messages. Security event: Details important actions and events in the diagnostics buffer which can trigger group alarms. External load memory: Allows for the disabling of copying from internal to external load memory.
OPC UA	Enables access to the PLC as an OPC UA server and allows for the configuration of security settings through security policies and certificates on the server.
System power supply (Page 169)	Enables automatic calculation of power consumption by providing an overview of power segments representing each configured module.
Advanced configuration	Contains: • Hostname and domain - Assign the name or IP address of the host computer and activate the domain configuration in STEP 7. • DNS configuration (Page 214) - Configure the DNS server address. • SNMP (Page 214) - Activate SNMP (Simple Network Management Protocol).
Connection resources (Page 218)	Provides a summary of the communication connection resources that are available for the CPU and the number of connection resources that have been configured.
Overview of addresses	Provides a summary of the I/O addresses that have been configured for the CPU.
Runtime licenses	Allows for the selection of runtime licenses that enable the CPU to act as an OPC UA server.

¹ If you disable access control, every user has full access to the CPU without a password. You are essentially granting users "Full access (no protection)" (if using a standard CPU) or "Full access incl. fail-safe (no protection)" (if using an F-CPU). Users can access most CPU functions. Because of this, Siemens recommends disabling access control only during commissioning and that only authorized persons have access to the CPU during this phase.

You can learn more about the above CPU properties by referring to the related device configuration topics in the TIA Portal Information System.

5.6.5.1 Configuring the system power supply

As you add modules to your configuration of the S7-1200 G2, TIA Portal automatically calculates your overall power consumption (Page 68). This enables you to anticipate the energy needs of a given physical device configuration.



You can configure the Sensor Supply wired interface to suit your application.

5.6.5.2 Pulse catch

The S7-1200 G2 CPU provides a pulse catch feature for digital input points. The pulse catch feature allows you to capture high-going pulses or low-going pulses that are of such a short duration that they would not always be seen when the CPU reads the digital inputs at the beginning of the scan cycle (Page 101).

Enabling pulse catch

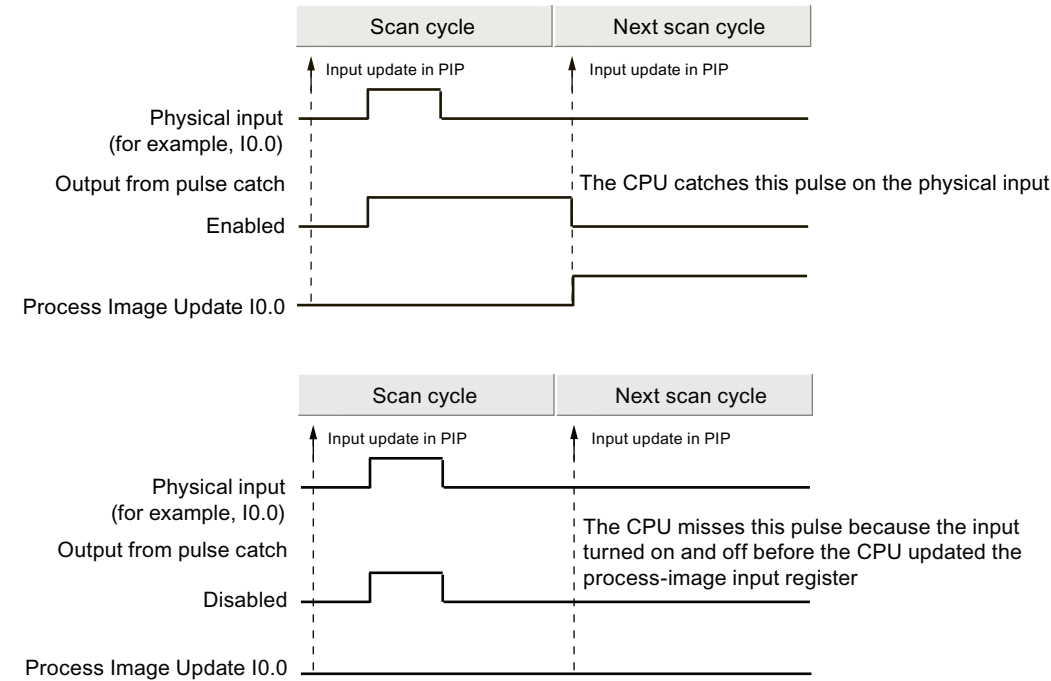
To enable pulse catch for a digital input, follow these steps:

1. Select "Digital inputs" in the Inspector window.
2. Select the desired channel.
3. Select "Enable pulse catch."

Basic operation of pulse catch

When you enable pulse catch for an input, a change in state of the input is latched and held until the next input cycle update. This ensures that a pulse that lasts for a short period of time will be caught and held until the CPU reads the inputs.

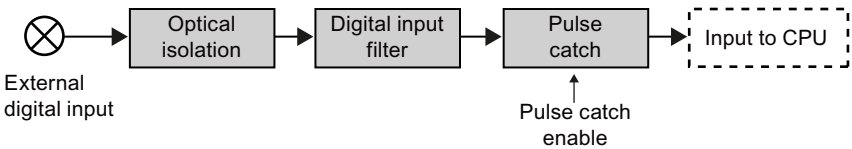
The figures below show the basic operation of the S7-1200 G2 CPU with and without pulse catch enabled:



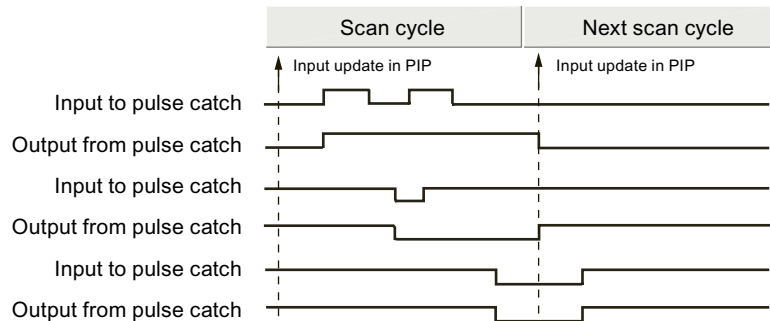
NOTE

Because the pulse catch function operates on the input after it passes through the input filter, you must adjust the input filter time so that the filter does not remove the pulse.

The figure below shows a block diagram of the digital input circuit:



The figure below shows the response of an enabled pulse catch function to various input conditions. If you have more than one pulse in a given scan, only the first pulse is read. If you have multiple pulses in a given scan, you should use the rising/falling edge interrupt events:



5.6.6 Configuring the parameters of the modules

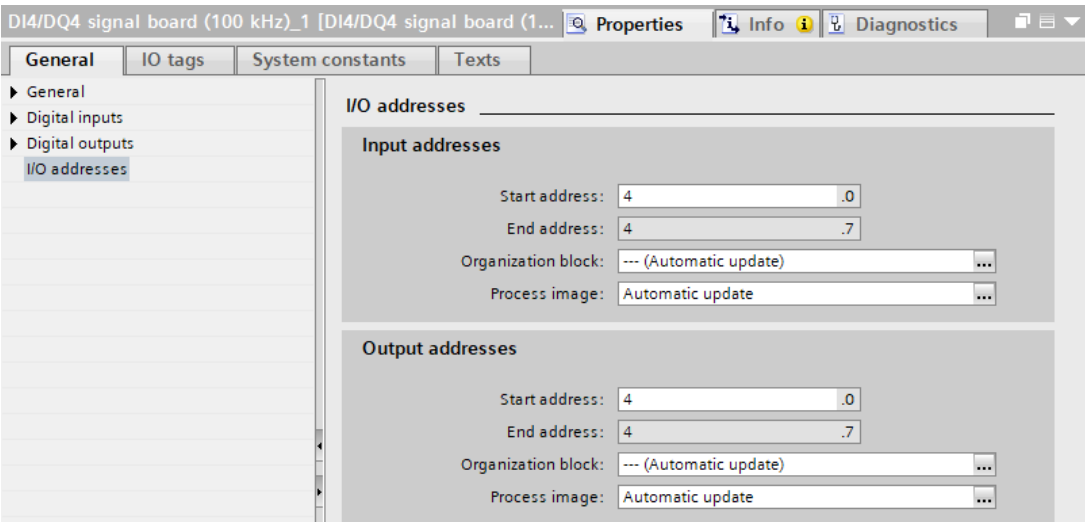
STEP 7 enables you to configure the inputs and outputs of devices connected to your S7-1200 G2 CPU on the network. You can assign values to both analog and digital I/O to accomplish tasks such as "pulse catch", to update process image partitions, or to monitor diagnostic functions.

To configure the operational parameters for the modules, select the module in the Device view and use the "Properties" tab of the inspector window.

Configuring a signal module (SM) or a signal board (SB)

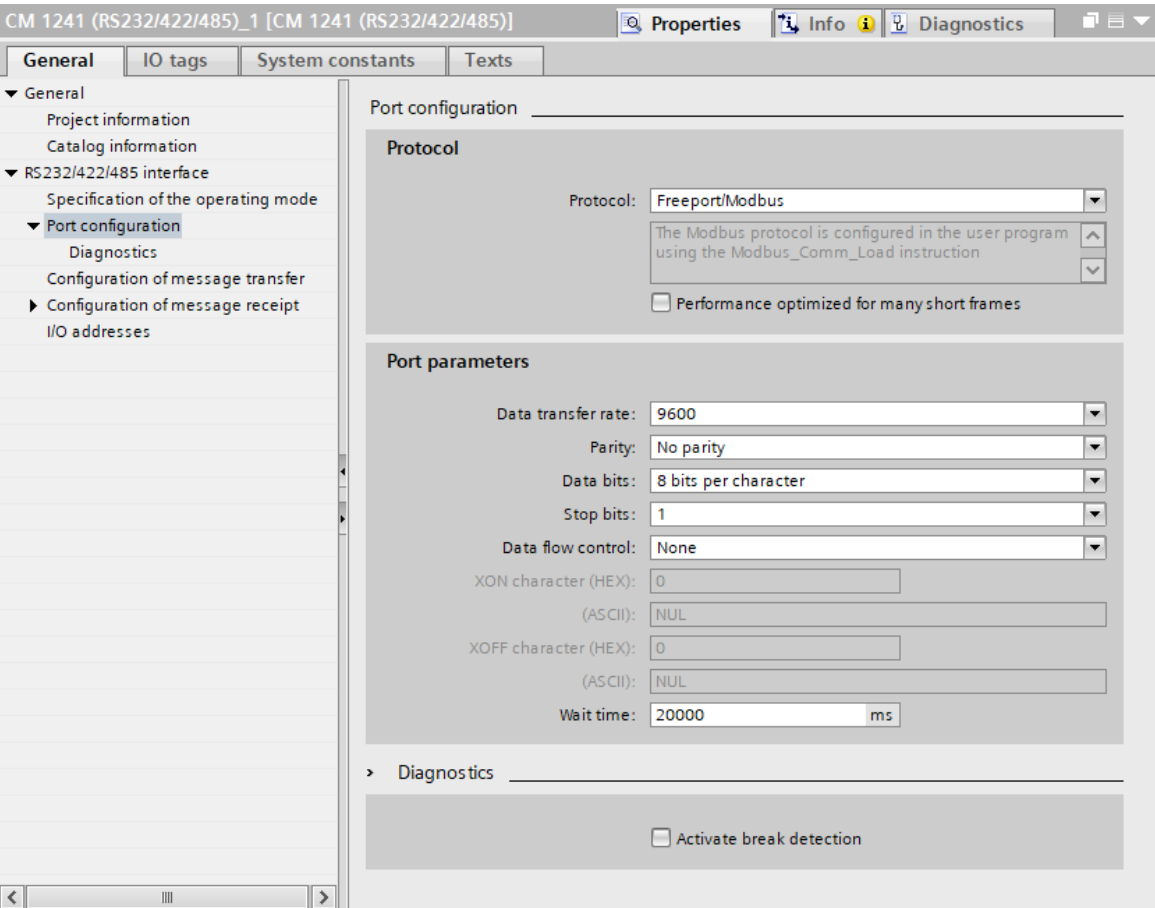
The device configuration for signal modules and signal boards provides the means to configure the following:

- **Digital I/O:** You can configure inputs for rising-edge detection or falling-edge detection (associating each with an event and hardware interrupt) or for "pulse catch" (to stay on after a momentary pulse) through the next update of the input process image. Outputs can use a freeze or substitute value.
- **Analog I/O:** For individual inputs, you can configure parameters such as measurement type (voltage or current), range, and smoothing, as well as enable underflow or overflow diagnostics. Analog outputs provide parameters such as output type (voltage or current) and for diagnostics, such as short circuit (for voltage outputs) or upper/lower limit diagnostics. You can configure the ranges of analog inputs and outputs in engineering units in your program logic.
- **I/O addresses:** You can configure the start address for the set of inputs and outputs of the module. You can also assign the inputs and outputs to a process image partition (PIP) or to automatically update, or to use no process image partition. See "Execution of the user program" (Page 101) for an explanation of the process image and process image partitions.



Configuring a communication module (CM)

You can configure the parameters for point-to-point communication modules (CMs) on the network.

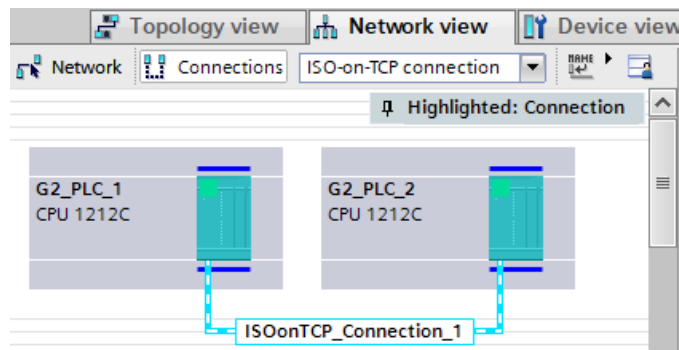


5.6.7 Configuring the CPU for communication

The S7-1200 G2 is designed to solve your communications and networking needs by supporting both simple and complex networks. The S7-1200 G2 also provides tools that allow you to communicate with other devices, which might use their own communications protocols.

Creating a network connection

Use the "Network view" of Device configuration to create the network connections [\(Page 222\)](#) between the devices in your project. After creating the network connection, use the "Properties" tab of the inspector window to configure the parameters of the network.



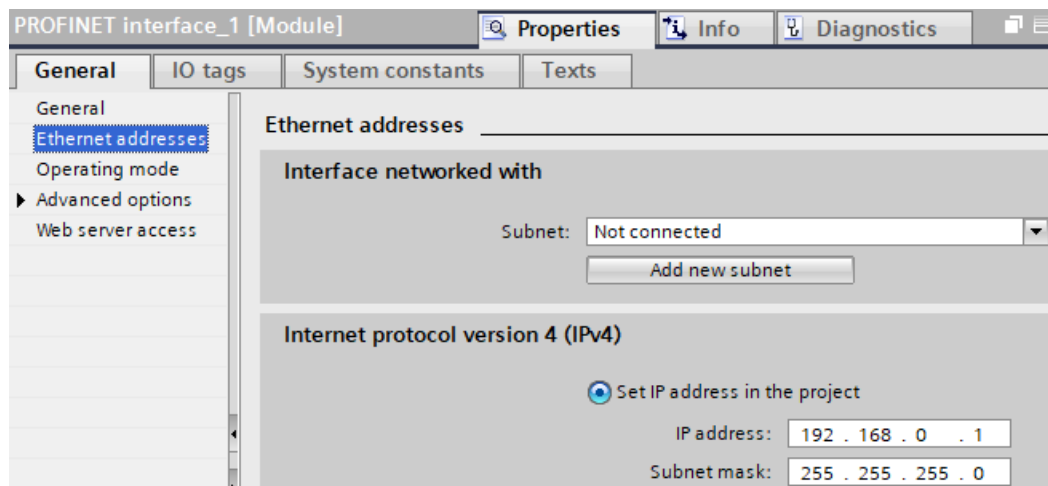
The S7-1200 G2 CPU supports the following connections:

- S7 connection [\(Page 267\)](#)
- ISO-on-TCP connection [\(Page 236\)](#)
- TCP connection [\(Page 236\)](#)
- UDP connection [\(Page 237\)](#)
- HMI connection (PLC to an HMI) [\(Page 246\)](#)

Assigning the IP address and Subnet

The S7-1200 G2 CPU does not have a pre-configured IP address. You must manually assign an IP address ([Page 227](#)) for the CPU in the Properties Tab under "General > Ethernet addresses".

To make a connection to your CPU, your chosen network interface and the CPU must be on the same class of network and on the same subnet. You can either set up your network interface to match the default IP address of the CPU, or you can change the IP address of the CPU to match the network class and subnet of your network interface.

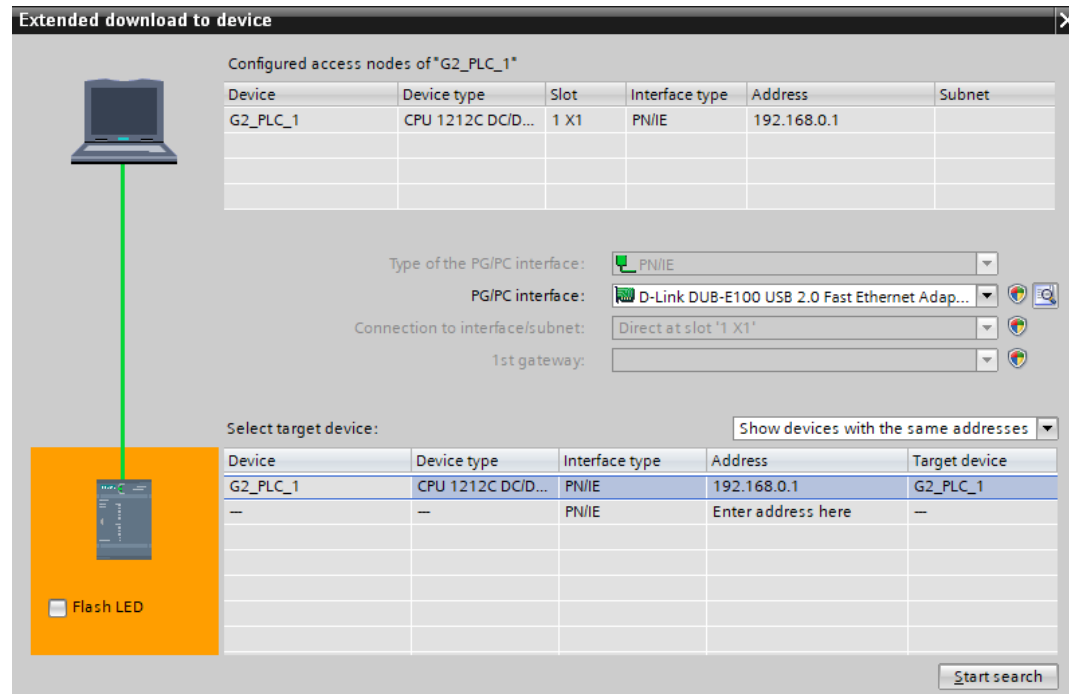


Configuring the Local/Partner connections

For the TCP, ISO-on-TCP, and UDP Ethernet protocols, use the "Properties" of the instruction (TSEND_C, TRCV_C, or TCON) to configure the "Local/Partner" connections ([Page 223](#)).

Downloading to the CPU

After configuration, download your STEP 7 project to the CPU to test the PROFINET network (Page 233). The download operation sets all IP addresses for devices configured as "Set IP address in the project".



5.6.8 Time synchronization

The objective of time synchronization of the time-of-day clocks is to have one master clock that synchronizes all other local clocks. The master clock synchronizes the local clocks initially and also periodically re-synchronizes the clocks to avoid the effects of drift over time.

In the case of the S7-1200 G2 and its local base components, only the CPU has time-of-day clocks that might need to be synchronized. You can configure the CPU's time-of-day clock to be synchronized to an external master clock. The external master clock might supply the time of day using an NTP server.

Setting the time-of-day clock

There are multiple ways to set the time-of-day clock in the S7-1200 G2 CPU:

- Using the NTP server (Page 235)
- Using STEP 7
- From the user program
- Using an HMI panel
- From the SIMATIC Automation Tool
- From the Web server

By default, time synchronization using the NTP server to change the CPU's clock is disabled.

You can select the update interval using the NTP server. The update interval of the NTP server is set to 10 seconds by default.

When you activate time synchronization in a module, STEP 7 prompts you to select the "CPU synchronizes the modules of the device", if you have not already selected the check box in the CPU's "Time synchronization" dialog. STEP 7 also warns you if you configured more than one master clock source for time synchronization.

**WARNING****Risk of attacker accessing your networks through open interfaces**

If an attacker can access your networks through open interfaces, such as software like STEP 7 or SAT, or through an HMI, the attacker can possibly disrupt control of your process by shifting the CPU system time.

The S7-1200 G2 CPU supports "time of day" interrupts and clock instructions that depend upon accurate CPU system time. You must restrict access to the CPU by enabling access control and disabling the "Anonymous" user. Failure to do so can cause a security breach that allows an unknown user to disrupt control of your process by shifting the CPU system time.

Disruptions to process control can possibly cause death, severe injury, or property damage.

For security information and recommendations, see the "Operational Guidelines

(<https://www.siemens.com/global/en/products/services/cert/news/operational-guidelines-for-industrial-security.html>)" white paper on the Siemens Industrial Cybersecurity Website.

NOTE

Receiving time synchronizations for the CPU from more than one source could cause conflicting time updates. Time synchronizations from multiple sources could adversely affect instructions and events based on time of day.

5.7 Compatibility between STEP 7 versions and the S7-1200 G2 CPU

TIA Portal versions V20 and later support configuration and programming of the S7-1200 G2 CPU. Older versions of the TIA Portal do not support the S7-1200 G2 family.

Working with an older project and adding S7-1200 G2 CPUs

You might want to add S7-1200 G2 CPUs to an existing application that uses other CPUs and that was created in an older version of the TIA Portal. To do this, you will need a TIA Portal V21 project.

You can open a V14 or later project in the latest version of the TIA Portal and upgrade the project to the latest TIA Portal version. The TIA Portal dialogs guide you in upgrading the project if it is possible. You can then add the S7-1200 G2 CPUs for your application and perform these tasks in the TIA Portal:

1. Configure the S7-1200 G2 devices.
2. Program the logic for the S7-1200 G2 CPUs.
3. Download the hardware configuration and software to the S7-1200 CPUs.

WARNING

Risks with editing and executing program logic from versions older than TIA Portal V13

Do not attempt to upgrade a project that is older than V14 to the current version by copying program logic from one CPU to an S7-1200 G2 CPU.

You must first open the older project in TIA Portal V14 and upgrade the project to V14. Then you can open the latest version of the TIA Portal and upgrade the project from V14 to the current TIA Portal version.

Executing STEP 7 program logic that you copied from an older version to a newer version can cause unpredictable program behavior and can result in death or severe personal injury.

Migrating program logic from an S7-1200 CPU to an S7-1200 G2 CPU

If you want to migrate existing program logic from an S7-1200 CPU to an S7-1200 G2 CPU, note that there is no device exchange from any type of CPU to an S7-1200 G2 CPU. Note also that the instruction set and library support in S7-1200 G2 has differences from other CPU families. To migrate program logic from an S7-1200 CPU to an S7-1200 G2 CPU, follow these steps:

1. Add an S7-1200 G2 CPU to the upgraded project that has S7-1200 CPUs and configure the device. Be sure to observe the Warning above when upgrading a project.
2. Copy the program blocks (Page 99) from the S7-1200 CPU to the program blocks of the S7-1200 G2 CPU.
3. Create and edit any PLC tag tables that you need.
4. Attempt to compile the program, choosing "rebuild all" for both hardware and software.
5. Resolve any memory and I/O addressing differences between the two CPUs. Resolve any instruction differences between the two CPUs. Continue resolving compiler errors until the program compiles.

TIA Portal Add-ins (<https://support.industry.siemens.com/cs/us/en/view/109773999>) might also be useful in program migration.

5.8 Instruction set

5.8.1 Supported programming languages

STEP 7 provides the following standard programming languages for the S7-1200 G2:

- LAD (ladder logic) is a graphical programming language. The representation is based on circuit diagrams.
- FBD (Function Block Diagram) is a programming language that is based on the graphical logic symbols used in Boolean algebra.
- SCL (structured control language) is a text-based, high-level programming language.
- CEM (Cause-Effect-Matrix) for programming Function Blocks (FBs)

When you create a code block (Page 99), you select the programming language for that block.

The STEP 7 program can utilize code blocks created in any or all of the programming languages.

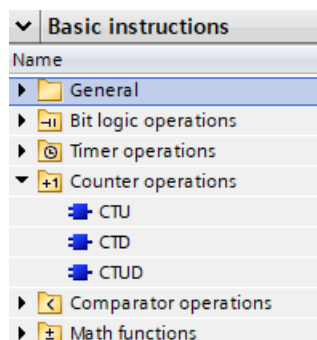
See the STEP 7 Information System for information on any of the programming languages.

5.8.2 Instructions for programming the PLC

STEP 7 provides instructions to program your S7-1200 G2 PLC. Categories and folders differ based on your programming language. The LAD Programming language presents instructions in the following main categories:

- Basic
- Extended
- Technology
- Communication
- Optional Packages

Folders under each main category list the instruction group as shown in the example below:



To find more information about each instruction and its use, follow these steps:

1. Open a program block to display the Instruction task card.
2. Expand an instruction group.
3. Do one of the following:
 - Select the individual instruction and press F1.
 - Hover over an individual instruction to reveal a TIA Portal tooltip. If you click the tooltip, or continue to hover over the instruction, a cascading tooltip provides a link to the corresponding instruction topic in the TIA Portal Information System.

You can access the TIA Portal Information System in one of the following ways:

- Select "Help" in the Portal view.
- Select the "Help > Show help" menu command in the Project view.

There you can find information on programming and instructions

(https://docs.tia.siemens.cloud/access?ft:originId=../16544462091/16544462091_enUS.htm&ft:clusterId/16544462091/16544462091.htm).

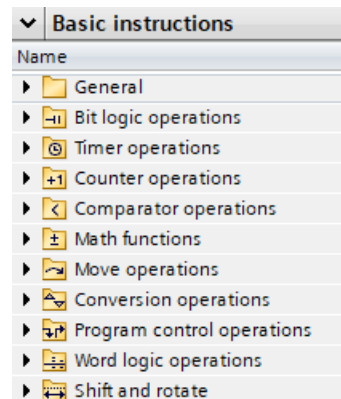
NOTE

Choosing an instruction by PLC family

If the TIA Portal Information System presents an instruction differently within the tooltips or table of contents based on PLC family, follow the S7-1500 option for the instruction topic.

5.8.3 Basic instructions

Basic Instructions are instructions that you use often and include the following folder groups:



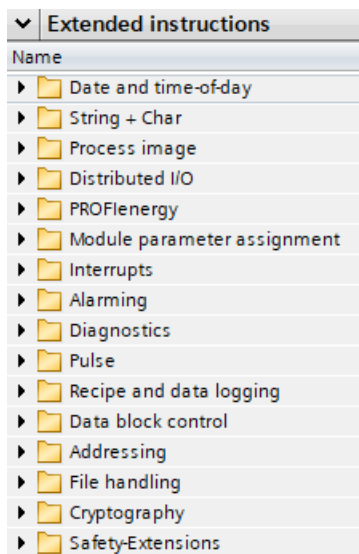
Instructions in these folders allow you to do the following:

- General - Add a network and connect network elements.
- Bit logic operations - Perform Boolean logic.
- Timer operations - Delay actions and measure elapsed time.
- Counter operations - Count internal program or external process events.
- Comparator operations - Compare two values or compare a value with a range and use the compare result in Boolean logic.

- Math functions - Perform calculations including integer and floating-point math.
- Move operations - Copy data elements to a new memory address and convert from one data type to another.
- Conversion operations - Convert from one data type to another, perform scaling, and round a floating-point number to the nearest integer.
- Program control operations - Control program sequence including jumps, retrigger cycle monitoring timer, and STOP the PLC.
- Word logic operations - Compare two values, bit by bit, using Boolean logic.
- Shift and rotate - Shift or rotate a value right or left by a specified number of bits.

5.8.4 Extended instructions

Extended instructions allow for more possibilities and include the following folder groups:



Instructions in these folders allow you to do the following:

- Date and time-of-day - Manipulate and compare time values. Set and read local time and system time.
- String + Char - Create, convert, and manipulate strings and characters. Search for, replace, insert, or append substrings.
- Process image - Update or synchronize the process image inputs or outputs.
- Distributed I/O - Exchange information with distributed I/O using read and write records.
- PROFlenergy - Activate or deactivate energy-saving states in lower-level PROFlenergy devices.
- Module parameter assignment - Read and write parameter records to modules.
- Interrupts - Control runtime aspects of interrupt events. Attach and detach OBs to interrupt events.
- Alarming - Generate program alarms and user diagnostic alarms.

- Diagnostics - Read status and diagnostic information. Generate diagnostic information for third-party components.
- Pulse - Control pulse width modulation (PWM) and pulse train output (PTO) functions.
- Recipe and data logging
 - Import and export recipes
 - Create, open, write, clear, close, and delete data logs (See "Working with data logs" below.)
- Data block control - Create a new data block in load or work memory. Transfer data between data blocks.
- Addressing - Convert module addresses among these options:
 - IO address
 - Hardware identifier
 - Slot
- File handling - Create a file on a memory card; write to and read from this file.
- Cryptography - Generate a random number. Perform encoding and decoding.
- Safety-Extensions - Acknowledge warning message about exceeding the F-cycle time.

Working with data logs

The TIA Portal Information System documents data logging at this path: Information System > Programming a PLC > Instructions > Instructions (S7-1200, S7-1500) > Extended instructions > Recipes and data logging > Data logging

In addition, be aware of this information when working with data logs:

NOTICE

Recommended frequency for write operations when using data logs

When using data logs in internal or external load memory, a high frequency of write operations can affect the S7-1200 system negatively.

To ensure the overall performance and robustness of your system, limit write operations to every 200 ms or longer.

Exceeding this limit can shorten the lifespan of the memory card or internal flash.

NOTE

Data log management

Keep no more than 1000 data logs in a file system. Exceeding this number can prevent the Web server from having enough CPU resources to display the data logs.

Manage your data logs to ensure that you only keep the number that you need to maintain, and do not exceed 1000 data logs.

NOTE**Editing data logs on the memory card**

You can copy data logs from a memory card using a PC card reader. Do not change them or delete them using a PC card reader.

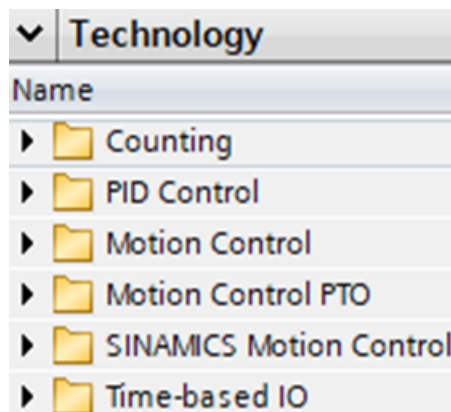
To delete, download, or display data logs use one of the following methods:

- SIMATIC Automation Tool
- DataLogDelete instruction
- Web API ([Page 316](#)) methods "DataLogs.DownloadAndClear", "Files.Browse", "Files.Download" and supporting code as documented for displaying data logs.

If you open the file system of the memory card in the File explorer, you run the risk of accidentally deleting or changing a data log or other system files, potentially damaging files or making the memory card unusable.

5.8.5 Technology instructions

Technology Instructions allow you to perform technological functions and include the following folder groups:

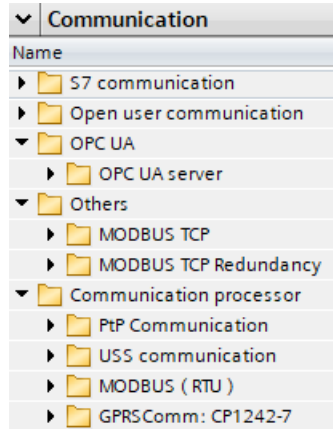


Instructions in these folders allow you to do the following:

- Counting - Control high-speed counter (HSC) functions such as counting and frequency measurement.
- PID Control - Control proportional-integral-derivative (PID) functions.
- Motion Control - Initiate absolute or relative moves. Perform homing and jog operations.
- Motion Control PTO - Power, reset, move, halt, home, and manage parameters for motion axes controlled via Pulse Train Output (PTO).
- SINAMICS Motion Control - Control stepper motors and servo motors. Coordinate motion axes.
- Time-based IO - Precisely monitor digital input state changes. Precisely control digital output state changes.

5.8.6 Communication instructions

Communication Instructions provide for communication using various network protocols and include the following folder groups:

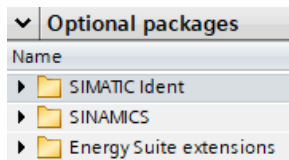


Instructions in these folders allow you to do the following:

- S7 Communication – Read data from or write data to a remote CPU using S7 protocol.
- Open user communication - Establish and terminate communication connections, send and receive data, send emails.
- OPC UA (server) - Define custom logic and actions that execute before and after a client calls an OPC UA server method.
- Others -
 - MODBUS TCP - Exchange data using Modbus TCP protocol (client or server) over the PROFINET interface.
 - MODBUS TCP Redundancy - Establish and manage redundant TCP communication connections between clients and servers.
- Communication Processor - Control serial communications such as point-to-point (PtP), Universal Serial Interface Protocol (USS), and Modbus Remote Terminal Unit (Modbus RTU).

5.8.7 Optional instructions

Optional Instructions provide additional functionality and include the following folder groups:



Instructions in these folders allow you to do the following:

- SIMATIC Ident - Interface with Siemens radio-frequency (RF) and optical identification systems.
- SINAMICS - Control Siemens variable-frequency drives (VFD).
- Energy Suite extensions - Calculate energy data. Create an energy report as a data log.

Protection

6.1 Overview of the protection functions

Advantages and customer benefits of protection functions

The protection functions listed protect your investments from unauthorized access and manipulation, helping to secure plant availability.

Protection functions

To set up secure networks, the SIMATIC S7-1200 G2 automation system offers an integrated security concept:

Table 6-1 Overview of protection functions

Protection function	Description
Integrity protection	The CPUs come with integrity protection functions as standard. These help detect any manipulations in the following: • Engineering data on the SIMATIC Memory Card • Engineering data during data transfer between TIA Portal and CPU • Engineering data during data transfer between HMI system and CPU • Encrypted firmware
Protection of confidential configuration data	Protection of confidential CPU configuration data (https://docs.tia.siemens.cloud/access?ft:originId=../10866368523/141646478219_enUS.htm&ft:clusterId./10866368523/141646478219.htm)
Central user management	Connection of a central server (UMC server) that is responsible for the administration and authentication of users. The central user management UMC (User Management Component) allows management of user groups and users independently of TIA Portal for extensive automation solutions.
Local user management	Management of users, roles, and CPU function rights (User Management & Access Control, UMAC). You can use the local user management in the editor to manage all project users along with their rights, including access rights for project users and roles in the TIA Portal.
Access protection	Protection against unauthorized configuration changes using authorization levels
Know-how protection	Protection against unauthorized access and modifications to algorithms with password protection

You can find more information about security mechanisms of the SIMATIC automation systems in the Communication Function Manual

(<https://support.industry.siemens.com/cs/ww/en/view/59192925>).

Integrity protection of the SIMATIC Memory Card

Integrity protection of the SIMATIC Memory Card depends on the password for protecting confidential configuration data that you assigned during the configuration of the CPU. This results in the following changes when using SIMATIC Memory Cards:

- To transfer a CPU to a card reader/USB memory device with drag and drop:
You must enter the password of the CPU you want to use with the SIMATIC Memory Card. If you enter an incorrect password, the CPU does not start booting after power on and reports the content of the SIMATIC Memory Card as faulty.
- To insert a CPU from a card reader/USB memory device:
You must enter the password of the CPU from which the project was loaded. In this case, STEP 7 checks the data on the SIMATIC Memory Card and reports potential damage.
Entering the password is optional. If you do not want to use the integrity check, you do not need to enter the password to restore the project.

You can select whether you also want to protect the entire configuration of the CPU in addition to protecting the configuration data. The data is encrypted and stored in the SIMATIC.S7S folder on the SIMATIC Memory Card and can only be decrypted with the password for the protection of confidential configuration data.

If you remove or add the setting for the protection of all data, the SIMATIC.S7S folder on the SIMATIC Memory Card remains formatted the next time it is loaded onto the CPU. Other files, for example, recipes or backup files on the SIMATIC Memory Card, are not formatted. After formatting, the CPU performs a restart.

You can find more information about the folder structure on the SIMATIC Memory Card in the "Structure and use of the CPU memory (<https://support.industry.siemens.com/cs/ww/en/view/59193101>)" Function Manual.

Secure communication

There is an increasing need to transfer data to external computers in encrypted form via Intranet or public networks.

SIMATIC S7-1200 G2 CPUs support the Internet PKI (RFC 5280) with STEP 7. This makes the configuration and the operation of secure communication possible, for example:

- Hypertext Transfer Protocol Secure (HTTPS)
- Secure Open User Communication
- Secure communication with OPC UA

A public key infrastructure (PKI) can issue, distribute, and check digital certificates. For S7-1200 G2 CPUs, you create certificates for various applications in the CPU properties in STEP 7, for example, TLS certificates for Secure Open User Communication, Web server certificates, or OPC UA certificates.

SIMATIC S7-1200 G2 CPUs, together with STEP 7 and WinCC, support innovative and standardized secure PG/PC and HMI communication.

Further measures for protecting the CPU

The following measures additionally increase the protection against unauthorized access to functions and data of the S7-1200 G2 CPU from external sources and through the network:

- Deactivation of the Web server
- Disabling the OPC UA server

You can find more information on the security mechanisms for OPC UA server in the Communication Function Manual (<https://support.industry.siemens.com/cs/ww/en/view/59192925>).

- Deactivation of the time synchronization via an NTP Server
- Deactivation of the PUT/GET communication
- Deactivation of SNMP

When you use the Web server, protect your S7-1200 G2 automation system against unauthorized access by doing the following:

- Set password-protected access rights for specific users in the user administration.
- Use the pre-set option "Permit access only via HTTPS".

The option allows access to the Web server only with the secure hypertext transmission protocol HTTPS.

When you use the OPC UA server, protect your S7-1200 G2 automation system against unauthorized access by doing the following:

- Do not set up OPC UA server access for the "Anonymous" user.
- Disable the "Automatically accept client certificates during runtime" option

Security functions in communications processors

Communication processors support security functions, such as access protection using a firewall, protection against data manipulation using VPN, FTPS, HTTPS, SNMPv3, and secure NTP.

More information

You can find more information on the protection functions described in the TIA Portal Information System.

Siemens products and solutions are only one element of a comprehensive industrial security concept. Observe the additional information on Industrial Security (<http://www.siemens.com/industrialsecurity>).

6.2 Protection of confidential configuration data

You can assign a password for protecting confidential configuration data of a CPU, such as private keys that are required for the proper functioning of certificate-based protocols.

You can find detailed information on protecting confidential configuration data in the Communication (<https://support.industry.siemens.com/cs/ww/en/view/59192925>) function manual.

6.3 Local user management

6.3.1 Useful information on the local user administration and access control

The S7-1200 G2 CPUs and TIA Portal provide management of users, roles, and CPU function rights (User Management & Access Control, UMAC).

You can manage all project users along with their rights, including access rights for all CPUs in the projects. In the TIA Portal, navigate to Security settings > Users and roles to manage users, role, and rights.

TIA Portal saves the assignment of the function rights of a CPU to user-defined roles and the assignment of these roles to users for each CPU. There are no system-defined roles with predefined function rights for CPUs.

After loading the configuration, the user management becomes effective in the respective CPUs. After loading, every CPU "knows" who may access which service and execute certain functions.

This new feature is also called "local user management and access control" below.

NOTE

Support of central users and groups for CPU function rights

UMC (User Management Component) can also be used to manage users ([Page 158](#)) centrally in TIA Portal. With this component, you can manage central users and groups on connected UMC servers, for example, by connecting an MS Active Directory. The authentication is then implemented via UMC.

User management as a component of your security strategy

Carefully designed user management increases the security of your automation solution, but only if you ensure the confidentiality of the user-relevant information.

In addition, the rules for industrial cybersecurity must be observed, for example regarding the "Defense in Depth" security concept, in particular the remarks on plant security and hardening measures.

You can find detailed information in the Industrial cybersecurity ([Page 22](#)) section.

Users, roles and function rights

Users and roles are managed in the TIA Portal under "Security settings > Users and roles".

CPU function rights are valid during runtime. These rights are located in the "Runtime rights" tab in the Users and roles editor. For each CPU in the project, there is a section for assigning CPU function rights, which are listed according to CPU services such as PG/HMI communication, Web server, and OPC UA.

In addition to user management for projects, user management possibilities are available for the following:

- OPC UA server users (authentication)
- Web server users (authentication and access control)

Local user management and access control

Use "Security settings > Users and roles" in the TIA Portal project tree to manage all users, roles, and CPU function rights. User management also enables you to set access protection [\(Page 191\)](#) for engineering/HMI access.

As with engineering rights, you use role assignments for combining individual function rights. You can assign these roles to individual users. You can see the function rights that are assigned to user from user roles for a specific CPU in the "Assigned rights" tab.

The following example shows the available and activated function rights of a CPU. At least one user must have full access to the CPU. Otherwise, the configuration cannot be compiled. A role with full access to the CPU must be created for this.

Roles				
	Name	Description	Runtime timeout	Comment
	NETDiagnose	System-defined role "NETDiagnose"	30 Min	
	Rol_PLC_1_Admin	User-defined role	30 Min 	Admin for PLC1 with Full Access
	<Add new role>			

Engineering rights

Runtime rights

User-specific runtime rights

Function rights categories		Function rights			
▼ Runtime rights			Name	Group	Comment
▼ S7-1200 G2 V1.0			Full access	Access level	
G2_PLC_1			HMI access	Access level	
▼ S7-1200 G2 V4.1			Read access	Access level	
G2_PLC_1			OPC UA server access	OPC UA	

In this example, the "PLC_1-Admin" user has a role ("Role_PLC_1-Admin") that provides full access to PLC "G2_PLC_1".

The screenshot shows the 'Users' configuration window with the 'Assigned roles' tab selected. The 'Assigned roles' table lists the roles assigned to the selected user.

Assigned to	Name	Description	Runtime timeout	Comment
☐	NET Standard	System-defined role "NET Standard"	30 Min	
☐	NET Diagnose	System-defined role "NET Diagnos..."	30 Min	
☒	Role_PLC_1-Admin	User-defined role	30 Min	Admin f

Requirement

To make use of users, roles and function rights for a CPU, the "Enable access control" option must be selected in the "Protection & Security > Access control" area.

In the "Configuration of user management" area, the "Local user management" option is preset, whereby the users are loaded to the CPU.

If you select the "Central user management" option, you must add additional parameters such as the UMC server address and server ID.

No project protection is required for user management [\(Page 158\)](#).

Default characteristics

The "Activate access control" option is preset for access control. Users can be configured with their assigned passwords and their roles and function rights.

Downloading to device

If you want to download changes to the user configuration in RUN mode, the hardware configuration in the CPU and in the STEP 7 project must be unchanged. Otherwise, a transition to STOP is required to download the user configuration together with the changed hardware configuration.

To download in RUN mode, save your STEP 7 project and then configure only the desired changes in the user configuration prior to loading the project into the CPU.

You can only download changes to access rights for the "Anonymous" user in STOP mode.

For an F-CPU, only a user with the runtime right "Full access incl. fail-safe (no protection)" can download a STEP 7 project. Otherwise, STEP 7 displays an error message when loading the configuration.

Explanations of the options for the user management download (Load preview):

- If you select the option "Keep online user management data", the local user management is not downloaded to the CPU.
- If you select the option "Download all user management data (reset to project)", all passwords changed online via WebAPI are deleted. After the download, the configured local user data is valid.
- If you select the option "Update user management data, but keep online passwords" and have not changed existing user names, the passwords changed online via WebAPI are retained. Only changes to function rights and/or roles take effect. Newly configured users are downloaded with their settings and deleted users are no longer available after the download to the CPU.

If you have changed a user name in the project and assigned a password to this user in the project, this setting becomes valid after the download. The previously valid user name in the online CPU is deleted during the download.

Runtime timeout

You can set a runtime timeout for both the role and the user in "Security Settings > Users and Roles".

For a S7-1200 G2 CPU, these settings are taken into account by the various services as follows:

- From the Web API you can, for example, create a Web page or application that takes the settings for the runtime timeout into account. Standard web pages do not take the settings for runtime timeout into account and use the default value.
- The other services (PG/HMI communication and OPC UA server) do not use the runtime timeout. The logged-in user is not logged out after the set time.

6.3.2 Advantages of the local user administration and access control

Quick activation/deactivation of local user management

The options for user administration are located in the "Protection & Security > Access control" tab:

- Access control deactivated: Every user has full access to all functions.

WARNING

Disabling access control

Disabling access control carries the risk of unauthorized access to the CPU.

Only disable access control in a protected environment, such as during commissioning.

Unauthorized access can cause death, personal injury, or property damage.

- Access control enabled: The configured users with their assigned roles and associated function rights become effective after loading.

Access protection and user authentication for PG/HMI access

In addition to assigning passwords for access levels for S7-1200 G2 CPUs, you can configure users with corresponding function rights for the CPUs.

In the TIA Portal project tree, you can configure protection for the project and password settings for runtime and engineering. From Security settings > Users and roles ([Page 158](#)), you can configure users for each CPU with designated roles and rights.

Powerful password functions

TIA Portal together with the CPU provide powerful password functions:

- Support for compliance with complexity rules for password creation:

At the password creation stage, you can have the TIA Portal check for compliance with complexity rules, such as rules on password length, uppercase/lowercase letters (project tree, "Security settings > Settings" area).

The complexity rules are also saved in the CPU when the user management is loaded.

When the password is changed online, the CPU determines and considers these rules. This prevents a user from overriding the complexity rules set by the configuration engineer and assigning a non-secure password.

- The period of validity of passwords is adjustable:

To ensure that a user does not have access to the CPU with a compromised password for an unlimited time, you can parameterize a period of validity. Before the period of validity expires, the remaining time is then displayed on login so that each user has the possibility to change their password in time.

Loading the user management during operation

You can load certain security-relevant configuration data in both STOP and RUN modes. This means that loading the hardware configuration does not necessarily lead to a CPU STOP.

You can download the following hardware configuration changes in STOP or RUN mode:

- Local user management extensions/changes
- TIA Portal-configured certificate modifications
- Syslog configuration changes

If you made additional changes to the hardware configuration (for example, modules added, parameters reassigned, or others), then the CPU automatically requests STOP mode before loading the configuration.

For example, if you load just one user with modified roles/function rights to the CPU, this process does not require the CPU to be in STOP mode.

The preview dialog for loading contains a security area so that you can determine how the CPU should deal with user data that has changed. (This is not applicable for loading for the first time). This allows changes to user data, for example, password changes during runtime, to be retained.

Loading the device as a new station - with user data

If you load a previously configured CPU into a new project, the user data is also loaded into the project and is available for further editing of the CPU settings.

Changing of passwords during operation

You can use the Web server API to write an application with which each user can change their password at runtime, provided that the original password was entered correctly and the new password corresponds to the password guidelines.

Requirement: You have enabled access control for the CPU.

Users can change their own password at any time, even if the password has expired. If the password has expired, the user must change the password. Login is not possible with an expired password.

API methods used:

- Api.ChangePassword
- Api.GetPasswordPolicy

You can find more information about the API methods in the Web server Function Manual (https://docs.tia.siemens.cloud/r/simatic_s7_1500_et_200mp_manual_collection_enus_20/comprehensive-information/cpu-function-manuals/web-server).

NOTE

Passwords changed at runtime take priority over loaded passwords

If you have changed your password during running operation and subsequently load your project, the password assigned during runtime takes precedence over the password set in the project (default setting).

If you want to overwrite the passwords changed during runtime by loading the project, you have to select the option "Load all user management data (reset to project data)". In this case, **all** passwords changed during runtime will be lost.

6.3.3 Access levels and function rights

Access levels as function rights

From the TIA Portal project, you can add users and roles ([Page 158](#)) with the necessary function rights for access control. The assignment between access level and the associated function right is as follows:

- Users who are to have full access must have a role with the function right "Full access", or "Full access incl. failsafe" for F-CPU.

You can only compile and load a CPU configuration if at least one user has the function right "Full access" or "Full access incl. failsafe".

- Users who are to have read access must have a role with the function right "Read access".
- Users who are to have HMI access must have a role with the function right "HMI access".

If a user does not have any of these specified function rights, that user has no access to the CPU.

Access levels also follow a hierarchical organization for the corresponding function rights:

- A user with "Full access incl. failsafe" also has "Full access".
- A user with "Full access" also has the function rights "Read access" and "HMI access".
- A user with "Read access" also has the function right "HMI access".

NOTE**Compatibility of the ENDIS_PW instruction**

The ENDIS_PW instruction

(https://docs.tia.siemens.cloud/access?ft:originId=../10867183243/52385784203_enUS.htm&ft:clusterId/10867183243/52385784203.htm) can only be used to disable or enable passwords for access levels. The ENDIS_PW instruction has no effect on assigned rights for users or roles. When using ENDIS_PW, take care to prevent users from being locked out of access to the CPU (Page 196). (Page 196)

Continuing to use access levels

You can use access level protection only. This is required, for example, for HMI devices that only support access levels and do not yet support assignment of users and roles.

If, for example, you require the configuration of an access level to ensure HMI device access, you must activate the "Use legacy access control via access levels" option in the CPU properties.

NOTE**Users for OPC UA and for the web server**

Independent of the access protection, you always have to configure the users (Page 158) for the Web server and OPC UA server.

Restrictions on continued use of the access levels

When using the "Legacy access control" option, you cannot select the access level directly in the table for setting the access levels. You can only set access protection via the function rights of the "Anonymous" user.

The local user "Anonymous" is created in a project by the system by default. With the "Anonymous" user, you determine the behavior of the CPUs in the project for someone who logs in without a user name and password. For security reasons, the Anonymous user is deactivated. You must activate it to use it.

In the CPU properties in the device configuration or in the security wizard when you add a CPU, you can access the editor to provide settings for the "Anonymous" user.

Examples:

- If the "Anonymous" user is deactivated or if the "Anonymous" user is activated and no function rights have been assigned to that user, then nobody can log in without a user name and password. This corresponds to the access level "No access (complete protection)".
- If the "Anonymous" user is activated and the "Full access" function right for a CPU is assigned to that user via a corresponding role, the result of this setting is "No protection". You can achieve the same effect with regard to access protection by setting "No access protection" in the "Protection & Security" area of the CPU properties.

Procedure

To activate the "Legacy access control" and set the required access level, follow these steps:

1. In the CPU properties, go to "Protection & Security > Access control".
2. Select the option "Activate access control" and, in addition, select the check box "Use legacy access control via access levels" check box.
The access level selection cannot be used in this setting. You have to set the access level via the "Anonymous" user of the CPU.
The "Anonymous" user is deactivated by default. This means that the resulting access level for users without a password is "No access (complete protection)" (default setting).
3. Go to "Security Settings > Users and roles" in the project tree.
4. Activate the "Anonymous" user if you want to set a different access level than "No access (complete protection)". You can assign a role with function rights that grants access to the CPU without password input, only to the activated "Anonymous" user.
5. You cannot assign function rights for a CPU directly to a user. You must first assign a role.

To assign a role, switch to the "Roles" tab and add a new role. Assign a meaningful name, for example, "PLC1-Read-Access-Role". If you assign this role to a user, this user should have read access to PLC1 during operation.

1. Assign the required function right for the access to the CPU with the name "PLC1" to the role "PLC1-Read-Access-Role", in this case "Read access".
2. Switch to the "User" tab and assign the "PLC1-Read-Access-Role" role to the activated "Anonymous" user.

Result: The "Anonymous" user has read access for PLC1. This means that the access level tables of the CPU "PLC1" in the project are preset to "Read access" (cannot be changed) and users who are not logged in only have read access.

For full access, or full access including fail-safe, you must configure a password for the full access in the table for the access protection. Users who need full access to the CPU during runtime via an action, for example, because a project is to be loaded onto the CPU, must legitimize themselves for this action with this password.

6.3.4 Important information when using the ENDIS_PW instruction

Using the ENDIS_PW instruction

(https://docs.tia.siemens.cloud/access?ft:originId=./10867183243/52385784203_enUS.htm&ft:clusterId./10867183243/52385784203.htm) to disable password access on the S7-1200 G2 CPU requires planning to prevent being locked out from CPU access. Because the S7-1200 G2 CPU does not have a display or keyswitch, like the S7-1500 CPU, if a reset of the CPU occurs where the startup state transitions to STOP mode, the ENDIS_PW instruction cannot run to re-enable passwords. This could cause users to be locked out of access to the CPU.

In versions 4.1 and later of the S7-1200 G2 CPU, existing password locks are removed during the transition from POWER OFF to POWER ON. This was not the case for V1.0.x versions where the passwords remained locked after POWER ON..

The S7-1200 G2 CPU applies configured passwords on power-up of the CPU. To have the passwords disabled after power-up, you must re-run the ENDIS_PW instruction to disable the passwords again.

Preventing unintentional lockout of an S7-1200 G2 CPU

Existing password locks are removed during the transition from POWER OFF to POWER ON of an S7-1200 G2 CPU. This means that it is possible and advisable to prevent unintentional lockout with the help of specific program sequences within your program.

To avoid unintentional lockout, program a time control with either a Cyclic interrupt OB or a timer in

OB 1. This gives you the option of calling the ENDIS_PW instruction in OB1 or the Cyclic interrupt OB relatively quickly after a transition from POWER OFF to POWER ON.

Call ENDIS_PW in the Startup OB to keep as short as possible the time window in which the application is not active and thus ensure that no restrictions exist in the password legitimization. This procedure offers you the greatest possible protection against unauthorized access.

If there has been an accidental lockout, you can omit the call in the Startup OB, by querying an input parameter, for example, and setting a time, for example, ten seconds up to one minute to establish a connection to the CPU before the lock becomes active once again.

If there is no timer in your program code and a lockout has occurred, follow the procedure below to recover from lost passwords.

Procedure for lost passwords with an S7-1200 G2 CPU

If you have lost the password for a password-protected S7-1200 G2 CPU, delete the password-protected program with an empty transfer card or program card. The empty transfer card or program card deletes the internal load memory of the CPU. You can then load a new user program from STEP 7 to in the CPU.

6.4 Central user management

6.4.1 Useful information on central user management and access control

S7-1200 G2 CPUs have a feature whereby authentication of users can be left to a central UMC server.

You manage users centrally and combine multiple users with the same roles/function rights into one group.

The central authentication service is performed by the UMC (User Management Component) (<https://support.industry.siemens.com/cs/us/en/view/109780337>).

You set up linking between user/group and assigned roles and function rights in the editor "Users and roles" ([Page 158](#)) in TIA Portal - as with the local user management.

User management as a component of your security strategy

Carefully designed user management increases the security of your automation solution, but only if you ensure the confidentiality of the user-relevant information.

In addition, you must observe the rules for industrial cybersecurity ([Page 22](#)), for example regarding the "Defense in Depth" security concept, and in particular the remarks on plant security and hardening measures.

Advantages of central user management

Central user management allows management of users and user groups independently of TIA Portal. This enables the user management to be scaled from a few users and CPUs in a single project (local user management) up to extensive automation solutions with multiple projects, users and user groups (central user management) without increased workload.

If you use the central user management (UMC), you can, for example, configure user groups on the UMC server set up for this purpose. The users of a group then have the same roles and function rights on the CPU.

During operation, users can be added to or removed from a group or passwords can be changed on the UMC server. The CPU configurations do not need to be changed and reloaded.

NOTE

Decoupling the user management from the CPU involves risks

When central user management is used, the CPU or TIA project has no way of checking the central user administration. UMC administrators must carefully check the effect of their changes with regard to modified roles and function rights.

Changes to central users at the time of the change do not affect the existing connection to the CPU. These include, for example, the following changes:

- Deletion of a user on the UMC server
- Moving users to other groups on the UMC server, which causes changes to roles and rights.

The changed user configuration only takes effect when you log in again.

Requirements

The Users and roles editor in the TIA Portal provides you with a wide scope of usage scenarios in connection with UMC:

- Programming device with TIA Portal that is connected to a UMC domain: In this case, the users and groups can be synchronized in the editor for users and roles.
- Programming device with TIA Portal that is not connected to a UMC domain but the names of the user groups/central users used in operation are known and can be added without contact to the UMC server:
 - The names of the user groups/central users can also be entered without connection to the UMC domain and synchronized with the UMC domain later.
 - Synchronization is not necessary for authentication of CPU users via a UMC server. The group names or user names only have to match to make use of the authentication service.

A CPU that needs to authenticate the querying users (for example, via web, PG/HMI communication, or OPC UA) for diverse online functions requires the following information for accessing the authentication service:

- The UMC server address
Example: `https://central.umc.testnet:443/ra`
(443 = Port for https, ra = remote authentication)
- A server ID (fingerprint of the server certificate).
You can determine the fingerprint of a certificate through Windows: (Open the certificate, "Details" tab, "Fingerprint" field).

As an alternative to the server ID, you can configure a list of CA certificates. These certificates are used by the CPU to verify the certificate returned by the UMC server when a connection is established. In order for the verification to be successful, the entire certificate chain down to the root certificate must have been loaded. The verification does not work for end-entity certificates or for intermediate certificates without a certificate chain to the root certificate.

Further requirements for operation during runtime are as follows:

- User groups and users have been set up on the UMC server.
- A connection can be established between the CPU and UMC server via the configured UMC server address.

- CPU time is current. As with local user management, central users are informed about the remaining validity of their password. CPU and UMC server must have the same date and time settings.

NOTE**No logon possible if the UMC server is not available or the CPU time is reset**

- If you use only UMC users and UMC user groups to access the CPU during operation and the UMC server becomes unreachable, for example, due to connection abort, then no one can log on anymore.
 - To enable access to the CPU in this case, configure at least one local user with the required roles/function rights.
 - If you use UMC user groups or UMC users to access the CPU during operation, the CPU time must be up-to-date.

If the CPU time has been reset, for example, by restoring the factory settings, and no NTP time synchronization has been configured, it is also not possible to log on via the central user management. Authentication of the UMC server using certificates requires an up-to-date CPU time.

 - To enable access to the CPU in this case, configure at least one local user with the required roles/function rights to set the time (for example, from the "Web server – Maintenance" group).
 - Alternatively, you can synchronize the CPU time using NTP servers [\(Page 175\)](#)
-

Basic procedure for using the User Management Component (UMC)

The following tasks are required to use the User Management Component (UMC):

1. Installation of UMC on one or more computers in the system
2. Assigning a corresponding UMC version as a UMC ring server or UMC server to create a UMC system consisting of one or multiple UMC computers.
3. Creating users and user groups in UMC: These can exist only in UMC or can be imported from a Microsoft Active Directory.
4. Connection of the UMC agent that is installed on the computer with the TIA Portal installation: The connection can be established with the TIA Administrator or with the Windows command line.
5. Use of UMC users and UMC user groups, for example, in the context of the TIA Portal project creation
6. Authentication of UMC users after logging on via UMC

NOTE**Enabled "Anonymous" user is always loaded**

An enabled "Anonymous" user with its configured roles/function rights is loaded even if you only enabled the central user management. Local user management does not have to be additionally enabled for the "Anonymous" user to take effect.

6.4.2 Configuring central user management in the editor for users and roles

The following procedures describe central user management in TIA Portal with an S7-1200 G2 CPU for the following use cases:

- The project is configured in the environment that has access to the UMC server.
- The project is created in an environment that has no access to the UMC server.

This is, for example, the case for a machine that is configured independently of the later place of installation and environment. The parameters for the user management must still be modified at the installation location.

Requirements - TIA Portal has access to the UMC server

- TIA Portal, editor for users and roles: The needed roles have been configured and the required function rights for these roles have been assigned.
- There is an online connection to the UMC server.

Procedure - Creating a new user group

To create a new user group, follow these steps:

1. Open the editor for users and roles (Project tree: Security settings > Users and roles).
2. Select the "User groups" tab.
3. Click the "Add new UMC user group" button.



4. Log on to the UMC server as the admin user.
5. In the dialog for selecting the user groups, select the user groups to be imported into the editor.
6. Assign the desired roles to the groups.

Procedure - Creating a new central user

To create a new central user, follow these steps:

1. Open the editor for users and roles (project tree: Security settings > Users and roles).
2. Select the "User" tab.
3. Click "Add user".



4. Log on to the UMC server as the admin user.
5. In the dialog for selecting the central users, select the users to be imported into the editor.
6. Assign the desired roles to the users.

Requirements - TIA Portal has no access to the UMC server

- TIA Portal, editor for users and roles: The needed roles have been configured and the required function rights for these roles have been assigned.
- There is no online connection to the UMC server at the time in which user management is configured.

NOTE**Case sensitivity of user name**

Although the UMC server does not differentiate between upper and lower case of the user name/group name when logging on, deviations in case prevent the user from logging on for users/groups configured offline or unsynchronized in the TIA Portal.

Recommendation:

- Before login, synchronize users and user groups in the TIA Portal and download this configuration to the CPU. In this practice, the case of the user name is not relevant during login.
 - If possible, import users/groups as described above.
-

Procedure - Creating a new user group

To create a new user group, follow these steps:

1. Open the editor for users and roles (project tree: Security settings > Users and roles).
2. Select the "User groups" tab.
3. Click in the <Add new user group> field in the "Name" column.

The TIA Portal enters a default name.

4. Modify the default name. This name will be used in the target environment of UMC.

The name can also be modified in the target environment during commissioning.

Result: The groups are set up but not synchronized, that is, no UM domain ID is assigned.

When a connection to the UMC server exists in the target environment, the following process takes place when a central user logs on:

- The CPU forwards the authentication request to the UMC server.
- After a successful check, the UMC server returns a list of groups to which the logged-on user belongs.
- The CPU determines the assigned roles and function rights for the user based on the group names.

Procedure - Creating a new central user

To create a new central user, follow these steps:

1. Open the editor for users and roles (project tree: Security settings > Users and roles).
2. Click in the <Add new user> field in the "User name" column.
The user type "Local user" is preset.
3. Modify the default user name - this name will be used in the target environment of UMC.
4. In the column "User type" change the entry to "Central user".

Result: The central user has been set up but not yet synchronized, meaning that no UM domain ID is assigned.

In the target environment with a connection to a UMC server, you can still adjust the provisional group and central user names using the TIA Portal.

Effects of changing the user type

- When you change the user type from central user > to local user, the data for the connection to the UMC server is lost.
- When the user type is changed from local user to a central user, the configured password and the comment are lost.

6.4.3 Configuring central user management for an S7-1200 G2 CPU

Procedure - CPU configuration for central user management

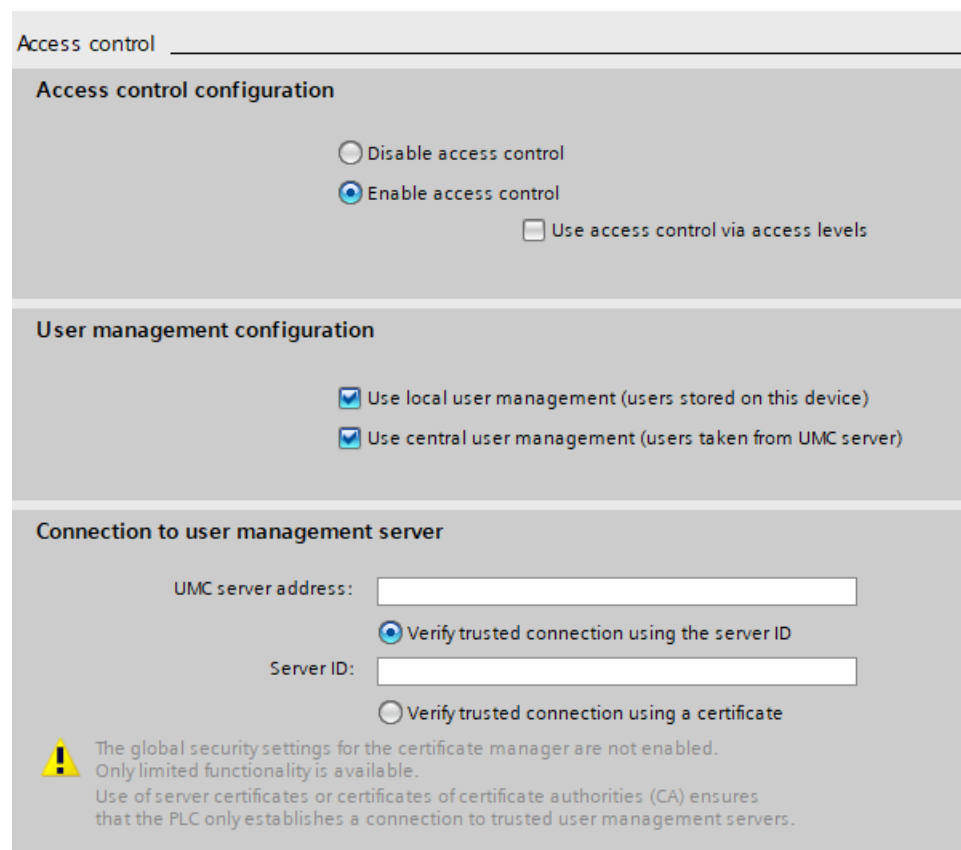
To configure the central user management for an S7-1200 G2 CPU, follow these steps:

1. From the properties of the CPU in Device configuration, navigate to "Protection & Security > Access control".
2. Ensure that access control has been enabled.
3. Activate the option "Use central user management (users taken from UMC server)".

In addition, you can also activate local user management to be able to access the CPU if, for example, the connection to the UMC server fails.

4. Add the specifications to the UMC server address and server ID for authentication of the UMC server.

As an alternative to the server ID, you can also add the CA certificate or intermediate certificate for authentication. The CPU must have the entire certificate chain for verification of the server certificate including root certificate.



Access control

Access control configuration

☐ Disable access control

☒ Enable access control

☐ Use access control via access levels

User management configuration

☒ Use local user management (users stored on this device)

☒ Use central user management (users taken from UMC server)

Connection to user management server

UMC server address:

☒ Verify trusted connection using the server ID

Server ID:

☐ Verify trusted connection using a certificate

 The global security settings for the certificate manager are not enabled. Only limited functionality is available. Use of server certificates or certificates of certificate authorities (CA) ensures that the PLC only establishes a connection to trusted user management servers.

Changing the connection data for the UMC server

A user with a role that grants full access to the CPU can download modified connection data (UMC server address and server ID) in both STOP and RUN modes of the CPU.

6.4.4 Logon of central users

The processes for the logon of central users are described below from the perspective of different applications.

Requirements

Requirements for logging on as a central user are as follows:

- A UMC server is connected to the CPU and is accessible.
- The required central users and groups have been set up for the UMC server.
- The CPUs are configured accordingly for the central user management (roles and function rights) and the configuration is loaded.

Logging onto a protected CPU

If you access a CPU online and the operation requires function rights, a dialog appears where you enter the user type. You can log on as a central user.

Causes of a failed logon of a central user

Common logon failures include the following:

- Entering an unconfigured or wrong user name
- Entering a wrong password
- A network problem such as the UMC server is not reachable or an oversized response frame

Tip: Set up a local user who can read the diagnostic buffer in the event of a failed logon and determine the exact cause. In the diagnostic buffer, the causes are represented by an error code that you can interpret using the following table. Each entry in the diagnostic buffer also leads to a corresponding syslog message so that connected evaluation systems can record the processes.

Table 6-2 Error codes for failed login

Error code	Meaning
#8000 0001	Missing configuration. The UMC server endpoint is not specified.
#8000 1000	Unspecified UMC system error.
#8000 1001	No DNS address configured.
#8000 1002	The DNS server is not reachable, for example, because it was shut down as the remote port is not reachable due to firewall settings.
#8000 1003	During data exchange with the UMC server: The interface is currently receiving new parameters.

Error code	Meaning
#8000 1004	The UMC server is not reachable. The UMC server does not respond to the ARP frame or there are problems with the TCP handshake to establish a connection.
#8000 1005	The IP address of the UMC server is not reachable due to missing routing information.
#8000 1006	The UMC server refuses to establish the connection. Connection was closed unexpectedly.
#8000 2xxx	Internal, unrecoverable TLS error.
#8000 3001	Validation of the UMC server certificate failed. Possible causes: Verification against the chain of trust not possible. Certificate not valid or expired. Verification of Identity failed (subject alternative name, FQDN, IPv4 check). Server ID verification failed (fingerprint).
#8000 4001	UMC server does not respond (timeout).
#8000 4002	HTTP response frame too long (system limit exceeded).
#8000 4003	Invalid HTTP response.
#8000 5xxx	Encoded HTTP status code of the HTTP request. Example of an encoding of Status Code 500 (#1F4) = Internal Server Error: Coding: #8000 5000 + #1F4 (=500) = #8000 51F4
#8000 6001	Syntax error in JSON response frame from UMC server.
#8000 6002	JSON response frame from the UMC server too long (system limit exceeded).
#8000 6003	Unexpected JSON format. The message has a valid JSON format, but it is not a valid UMC authentication response from the UMC server.
#8000 7xxx	Login failed (unknown error).

Logging on as an OPC UA client or as a Web client

When an OPC UA client logs on to the OPC UA server of the S7-1200 G2 CPU, the user name and password are transferred via the `UserNameIdentityToken`.

The user name and password are also queried for Web clients if you want to use the full functionality of the Web server

(https://docs.tia.siemens.cloud/r/simatic_s7_1500_et_200mp_manual_collection_enus_20/comprehensive-information/cpu-function-manuals/web-server). The following process applies to OPC UA clients and Web clients:

- For central users, the CPU forwards the authentication query to the UMC server.
- If the authentication is successful, the UMC server returns the assigned groups to which the user belongs.
- The CPU generates the corresponding session context and grants the authorizations (function rights from the determined roles).
- The client can then execute the access in the context of the session in accordance with the granted function rights.

How does the CPU (OPC UA server or the Web site of the Web server) detect whether the user is a local or central user?

You have the freedom to configure a user both as a local user and as a central user. This results in an ambiguity about which service is responsible for the authentication and which user ultimately gains access. Since access permission for the user depends solely on the password in this case, you should use strong passwords, for example, created by a password generator.

The following rules apply to ensure unambiguousness for the responsible authentication service (local or central user management):

- For logon of a local user, add the prefix "L:" (uppercase or lowercase) in front of the user name.
Example: L:username
- If you do not use a prefix for the user names, central user management is automatically responsible (when central and local user management are used at the same time). If you use only one type of user management, access is unambiguous even without a prefix.
- A user name must not begin with the string "L:" (uppercase or lowercase).

6.5 Configuring access protection for the CPU

Introduction

You can use the local user management (Page 188) in the editor for users and roles in the project tree. The access levels are represented there by function rights of the same name which you assign to individual users through their roles.

The CPU provides you with various access levels to limit access to specific functions.

By setting up access levels and passwords, you limit the functions and memory areas that are accessible without a password. The individual access levels and their associated passwords are specified in the object properties of the CPU.

Rules for passwords

Ensure that passwords are sufficiently secure by applying the following rules:

- Assign a password that is at least ten characters long.
- Use different cases and characters: uppercase/lowercase, numbers and special characters.

Passwords must not follow a machine-recognizable pattern.

Access levels of the CPU

Access levels	Access restrictions
Full access including fail-safe (no protection)	Users of STEP 7 and HMI applications have access to all standard and fail-safe functions. A password is not required.
Complete access (no protection)	Users of STEP 7 have access to standard functions. HMI applications can access all functions (fail-safe and standard). Additionally, to access the fail-safe functions, the user must enter the password for "Full access incl. fail-safe" in STEP 7.
Read access	In this access level, only read access to the hardware configuration and the blocks is possible without a password. HMI access and access to diagnostics data is also possible. You can download neither blocks nor the hardware configuration to the CPUs without the password. Additionally, you cannot write test functions or perform an online firmware update without the password.
HMI access	The access restrictions that apply to read access also apply to HMI access. Additionally, you cannot perform test functions, change the operating mode (RUN/STOP), perform a firmware update, or display an online/offline comparison status.
No access (complete protection)	When the CPU has complete protection, no read or write access to the hardware configuration and the blocks is possible (without access authorization in the form of a password). HMI access is also not possible. The server function for PUT/GET communication is disabled in this access level and cannot be changed. Authentication with the password provides you full access to the CPU.

An enumeration of which functions are available in the different access levels is available in "Setting options for the protection" in the TIA Portal Information System.

Properties of the access levels

Each access level allows unrestricted access to certain functions without entering a password, for example, identification using the "Accessible devices" function.

The default of the CPUs is "No access (complete protection)". In the default access level, the user can neither read nor change the hardware configuration or the blocks. To obtain access to the CPUs, use one of the following alternative parameter assignments in the properties of the CPU:

- A password for the protection level "No access (complete protection)"
- A different protection level, for example, "Full access (no protection)"

Communication between the CPUs, such as through the communication functions in the blocks, is not restricted by the access level of the CPU, unless PUT/GET communication is deactivated in the "No access (complete protection)" access level.

6.5 Configuring access protection for the CPU

Entry of the right password allows access to all the functions that are allowed in the corresponding level.

NOTE

Configuring an access level does not replace know-how protection

Configuring access levels offers a high degree of protection against unauthorized changes on the CPU through network access. Access levels are used to restrict the rights to download the hardware and software configuration to the CPU. However, blocks on the SIMATIC Memory Card are not write-protected or read-protected. Use know-how protection to protect the code of blocks on the SIMATIC Memory Card.

Behavior of functions with different access levels

The TIA Portal Information System contains a tabular list of the online functions that are possible in the various access levels.

Configuring access levels

To configure the access levels for an S7-1200 G2 CPU, follow these steps:

1. Open the properties of the S7-1200 G2 CPU in the Inspector window.
2. Open the "Protection & Security" entry in the area navigation.

A table with the possible access levels appears in the Inspector window.

More information about 'PLC access level'

Select the access level for the PLC.

Access level	Access				Access permission
	HMI	Read	Write	Fail-safe	Password
☐ Full access incl. fail-safe (no protection)	✓	✓	✓	✓	
☐ Full access (no protection)	✓	✓	✓		
☐ Read access	✓	✓			
☐ HMI access	✓				
☒ No access (complete protection)					

No access (complete protection):
TIA Portal users will not have access to standard functions or fail-safe functions.

Mandatory password:
For full access, TIA Portal users need to enter the "full access incl. fail-safe" password.

Optional password:
For read/write access to standard functions alone without access to fail-safe functions, a "read/write access" or "read access" password can be defined.

Some HMI devices do not support all possible characters. If you want to access the PLC from an HMI device, use only the standard characters. Please refer to the documentation of the device.

3. Activate the desired protection level in the first column of the table. The green check marks in the columns to the right of the respective access level show you which operations are still available without entering the password. In this example, access is not possible without a password.
4. In the "Access permission" column, specify a password for the access level "Full access" in the first row. In the "Confirm password" column, enter the selected password again to prevent incorrect entries.
5. Assign additional passwords as required for other access levels.
6. Download the hardware configuration for the access level to take effect.

The CPU logs the following actions with an entry in the diagnostic buffer:

- Input of the correct or incorrect password
- Changes to access level configuration

Behavior of a password-protected CPU during operation

Protection of an S7-1200 G2 CPU takes effect for an online connection after you have downloaded the settings to the CPU. If you set a higher access level and download it to the CPU, all other online connections are interrupted. You must then establish a new online connection.

Before an online function is executed, STEP 7 checks the necessary permission and, if necessary, prompts the user to enter a password. The functions protected by a password can only be executed by one programming device/PC at any one time. Another programming device/PC cannot log on.

Logon authorization to the protected data applies for the duration of the online connection or for as long as you have STEP 7 open. The menu command "Online > Delete access rights" cancels the access authorization.

Access level for F-CPUs

For fail-safe CPUs, there is an additional access level in addition to the four described access levels. For more information on this access level, refer to the description of the fail-safe system in SIMATIC Safety Programming and Operating Manual SIMATIC Safety - Configuring and Programming (<https://support.industry.siemens.com/cs/us/en/view/54110126>).

6.6 Know-how protection

Application

You can use know-how protection to protect one or more OB, FB or FC blocks as well as global data blocks in your program from unauthorized access. Enter a password to restrict access to a block. The password offers high-level protection against unauthorized reading or manipulation of the block. Know-how protection does not involve the CPU (offline access in STEP 7).

Password provider

As an alternative to manual password input, you can assign a password provider to STEP 7. When using a password provider, you select a password from a list of available passwords. When a protected block is opened, STEP 7 connects to the password provider and retrieves the corresponding password.

To connect a password provider you have to install and activate it. A settings file in which you define the use of a password provider is also required.

A password provider offers you the following advantages:

- The password provider defines and manages the passwords. When know-how protected blocks are opened, you work with symbolic names for passwords. For example, a password is marked with the symbolic name "Machine_1" in the password provider. The actual password behind "Machine1" remains hidden from you. A password provider therefore offers optimum block protection as the users do not know the password themselves.
- STEP 7 automatically opens know-how protected blocks without the direct entry of a password. This saves you time.

You can find more information on connecting a password provider in the STEP 7 online help.

Readable data

If a block is know-how protected, only the following data is readable without the correct password:

- Block title, comments and block properties
- Block parameters (INPUT, OUTPUT, IN, OUT, RETURN)
- Call structure of the program
- Global tags without information on the point of use

Further actions

Further actions that can be carried out with a know-how protected block:

- Copying and deleting
- Calling within a program
- Online/offline comparison
- Load

Global data blocks and array data blocks

You protect global data blocks (global DBs) from unauthorized access with know-how protection. If you do not have the valid password, you can read the global data block but not change it.

Know-how protection is not available for array data blocks (array DBs).

Setting up block know-how protection

To set up block know-how protection, follow these steps:

1. Open the properties of the respective block.
2. Select the "Protection" option under "General".

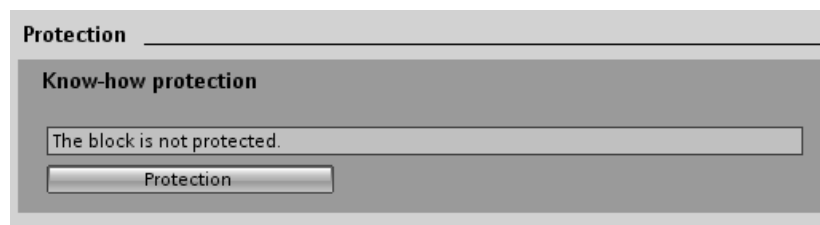


Figure 6-1 Setting up block know-how protection (1)

3. Click the "Protection" button to display the "Define protection" dialog.

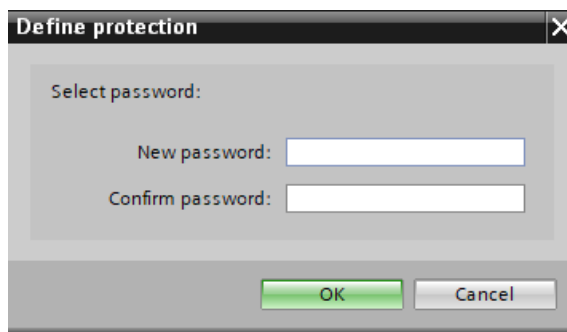


Figure 6-2 Setting up block know-how protection (2)

4. Enter the new password in the "New password" field. Enter the same password in the "Confirm password" field.
5. Click "OK" to confirm your entry.
6. Close the "Know-how protection" dialog by clicking "OK".

Result: The blocks selected will be know-how-protected. Know-how protected blocks are marked with a lock symbol in the project tree. The password entered applies to all blocks selected.

NOTE**Password provider**

Alternatively, you can set up know-how protection for blocks with a password provider.

Opening know-how protected blocks

To open a know-how protected block, follow these steps:

1. Double-click the block to open the "Access protection" dialog.
2. Enter the password for the know-how protected block.
3. Click "OK" to confirm your entry.

Result: The know-how-protected block opens.

Once you have opened the block, you can edit the program code and the block interface of the block for as long as the block or STEP 7 is open. You need to enter the password again the next time you open the block. If you close the "Access protection" dialog with "Cancel", the block will open but the block code will not be displayed. You will not be able to edit the block.

If you copy the block or add it to a library, for example, this does not cancel the know-how protection of the block. The copies will also be know-how-protected.

Changing know-how protection for blocks

To change the know-how protection for blocks, follow these steps:

1. Select the block for which you want to change the know-how protection. The protected block must not be open in the program editor.
2. To open the "Change protection" dialog, select the "Know-how protection" command in the "Edit" menu.
3. To change the password for the know-how protection, enter the current password under "Old password".
4. Then enter a new password under "New password" and confirm the password under "Confirm password".
5. Click "OK" to confirm your entry.

Result: The password for the know-how protection of the selected block has been changed.

Removing know-how protection for blocks

To remove block know-how protection, follow these steps:

1. Select the block from which you want to remove know-how protection. The protected block must not be open in the program editor.
2. Select the "Know-how protection" command in the "Edit" menu.

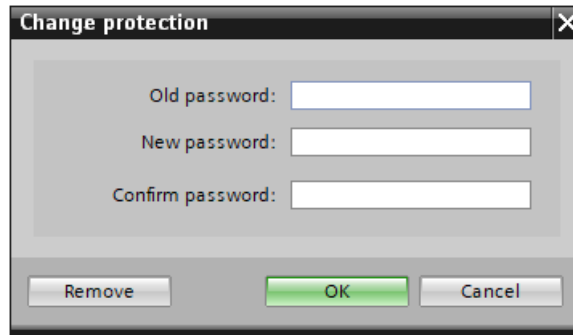


Figure 6-3 Removing know-how protection for blocks

3. To remove the block protection, enter the current password under "Old password". Leave the fields for the new password empty.
4. Click "Remove" to confirm your entry.

Result: Know-how protection for the selected block has been canceled.

6.7 Using the user program to set additional access protection

Access protection by means of the user program

In addition to access protection, you can also restrict access to a password-protected CPU using the `ENDIS_PW` instruction (https://docs.tia.siemens.cloud/access?ft:originId=../10867183243/52385784203_enUS.htm&ft:clusterId/10867183243/52385784203.htm) in STEP 7. When using `ENDIS_PW`, take care to prevent users from being locked out of access to the CPU (Page 196).

Communication

7.1 Overview

The S7-1200 G2 offers several types of communication between CPUs and programming devices, HMIs, and other CPUs.

PROFINET

PROFINET (<https://us.profinet.com/>) (PN) is used for exchanging data through the STEP 7 program with other communications partners through Ethernet.

For the S7-1200 G2, PROFINET supports 31 IO devices with a maximum of 512 submodules as well as the following:

- S7 communication ([Page 267](#))
- Open User Communication with the following protocols:
 - User Datagram Protocol ([Page 237](#)) (UDP)
 - ISO on TCP ([Page 236](#)) (RFC 1006)
 - Transport Control Protocol ([Page 236](#)) (TCP)
- PROFINET Security Class 1
(<https://support.industry.siemens.com/cs/ww/en/view/49948856/184125926283>)

PROFINET IO controller

As an IO controller using PROFINET IO, the CPU communicates with up to 31 PN devices on the local PN network.

CPU-to-CPU S7 communication

You can create a communication connection (https://docs.tia.siemens.cloud/access?ft:originId=./10866368523/34492344715_enUS.htm&ft:clusterId./10866368523/34492344715.htm) to a partner station and use the PUT and GET instructions ([Page 267](#)) to communicate with S7 CPUs.

Network security

WARNING

Avoiding security risks from network attacks

If an attacker can access your networks, the attacker can possibly read and write data.

For example, I/O exchange through PROFINET, PUT/GET (Page 267), T-Block, and communication modules (CMs) have no security features. You must protect these forms of communication.

If you fail to protect these forms of communication, death or severe personal injury can result.

For security information and recommendations, see the "Operational Guidelines

(<https://www.siemens.com/global/en/products/services/cert/news/operational-guidelines-for-industrial-security.html>)" white paper on the Siemens Industrial Cybersecurity Web site.

OPC UA server

S7-1200 G2 CPUs support configuration as an OPC UA server (Page 273) for data access. OPC UA clients can securely connect to the S7-1200 G2's OPC UA server to read or write the PLC data.

7.2 Secure communication

S7-1200 G2 CPUs implement secure communication between PLCs and the TIA Portal, SIMATIC Automation Tool, and HMIs. This implementation uses the industry standard TLS 1.3 (Transport Layer Security) protocol. The S7-1200 G2 CPU does not support legacy PG/PC communication.

Advantages of secure communication

Secure communication offers the following advantages:

- Confidentiality: Ensures that data remains confidential and cannot be accessed by unauthorized individuals.
- Integrity: Guarantees that the received message has not been modified during transmission.
- End point authentication: Verifies the identity of the communication partner.

Today, networked industrial machinery and control systems with sensitive data are at high risk and consequently pose high security requirements for data exchange.

Protection through firewall, VPN connection, or a security module, was common in the past and remains common. In addition to physical security, secure communication supports the transfer of data to external communication partners in encrypted form.

The CPU uses X.509 certificates (Page 220) to provide secure communication between the CPU and clients. Clients such as STEP 7 and the SIMATIC Automation Tool might require that you trust the certificate that is in the CPU. Be aware of the certificate you download to a CPU so that you can trust it when prompted.

Considerations when using secure communication

Communication speeds can be slower with secure communication.

- Actual firmware version of the physical CPU
- Configured firmware version (Page 177) of the CPU in the STEP 7 project

Additional information

You can find additional details about the implementation of secure communication in the TIA Portal Information System. In particular, additional information about certificates is in the following TIA Portal Information System topics:

- Confidentiality through encryption
- Managing certificates with STEP 7
- Examples for the management of certificates
- Authenticity and integrity through signatures

7.3 Communication protocols and ports used by Ethernet communication

The specified ports are the standard port numbers that the S7-1200 G2 CPU uses. Many communication protocols and implementations enable you to use other port numbers. The following tables show different layers, protocols, and ports used in the S7-1200 G2 CPU.

Table 7-1 Transport layer ports and protocols by S7-1200 G2

Port(s)	Direction	Protocol	Applica- tion	Description	Default setting/notes
25	Outbound	TCP	SMTP	SMTP is used for sending e-mails.	Default: Deactivated. Can be enabled via TMAIL_C instruction in the STEP 7 program.
68	Outbound	UDP	DHCP	The IP address suite is obtained from a DHCP server during the startup of the PROFINET interface.	Default: Deactivated. Can be changed in the CPU properties
102	Inbound/ Outbound	TCP	ISO-on-TCP	ISO-on-TCP (according to RFC 1006). The S7 protocol uses ISO-on-TCP according to RFC 1006 for PG/HMI communication with TIA Portal.	Default: Activated. This function cannot be deactivated.
123	Outbound	UDP	NTP	NTP is used for synchronization of the CPU system time with the time of an NTP server.	Default: Deactivated. Can be enabled in the CPU properties.
161	Inbound	UDP	SNMP	SNMP is used for reading and setting network management data (SNMP managed Objects) by the SNMP Manager.	Default: Deactivated. Can be enabled via data record in the STEP 7 project or in CPU Properties. Provides customizable community strings to limit access.
443	Inbound	TCP	HTTPS	HTTPS is used for secure communication with the CPU-internal web server over TLS.	Default: Deactivated. Can be enabled by enabling the Web server in the CPU properties.

7.3 Communication protocols and ports used by Ethernet communication

Port(s)	Direction	Protocol	Applica- tion	Description	Default setting/notes
465, 587	Outbound	TCP	SMTPS	SMTPS is used for sending e-mails over secure connections.	Default: Deactivated. Can be enabled via TMAIL_C instruction in the STEP 7 program.
502	Inbound/ Outbound	TCP	Modbus	Modbus/TCP is used by MB_CLIENT/MB_SERVER instructions in the STEP 7 program.	Default: Deactivated. Can be activated via Modbus instructions in the STEP 7 project. Port 502 is the default port for Modbus, but can be configured to other values via the Modbus instructions in the STEP 7 program.
4840	Inbound	TCP	OPC UA	Open Platform Communications Unified Architecture (based on TCP/IP protocol). A communication standard ranging from the enterprise level to the field level.	Default: Deactivated. Can be enabled in the CPU properties.
6514, 514	Outbound	TCP (6514) UDP (514)	Syslog Client	The Syslog client of the CPU is used for transferring syslog messages to a server.	Default: Deactivated. Can be enabled in the CPU properties. You can configure the forwarding of syslog messages to a syslog server in the CPU properties. The collection of system logging events within a CPU cannot be disabled. Port 6514 is the default value for Syslog servers in STEP 7. Port 514 is the standard port for UDP Syslog servers, but it is not the default value even if you select UDP in the STEP 7 project configuration.
34964	Inbound/ Outbound	UDP	PROFINET Context Manager	The PROFINET Context Manager provides an endpoint mapper in order to establish an application relation (PROFINET AR).	Default: Enabled (UDP port open). This function cannot be deactivated.

Table 7-2 Port ranges that could be used by Open User Communication (OUC) and other protocols.

Port Range	Direction	Protocol	Application	Description
1-1999	Varies	TCP/UDP	OUC	This port range can be used to limited extent, excluding already used ports.
2000-5000	Varies	TCP/UDP	OUC	This is the recommended port range for OUC.
5001-49151	Varies	TCP/UDP	OUC	This port range can be used to limited extent, excluding already used ports.
49152-65535	Outbound	TCP/UDP	Varies	This is the Dynamic port area used for active connection end point if the application does not determine the local port number.

You define these communication parameters in the STEP 7 program.

7.4 Asynchronous communication connections

Table 7-3 Protocols used by S7-1200 G2 in the Data Link and Network Layer (Layer 2, 3) of the OSI model.

Protocol	Direction	Ethertype	Description
PROFINET DCP	Inbound/Outbound	0x8892	DCP is used by PROFINET to discover PROFINET devices and provide basic settings. DCP uses the special multicast MAC addresses: 01-0E-CF-00-00-00 and 01-0E-CF-00-00-01.
LLDP	Outbound	0x88CC	LLDP is used by PROFINET to discover and manage neighbor relationships between PROFINET devices. LLDP uses the special multicast MAC address: 01-80-C2-00-00-0E.
PROFINET IO	Inbound/Outbound	0x8892	The PROFINET IO frames are used to transmit IO data cyclically between PROFINET IO controller and IO devices via Ethernet.
ICMP	Inbound	0x0800	Internet Control Message Protocol is used for diagnostic or control purposes.
MRP	Inbound/Outbound	0x88E3	Media Redundancy Protocol enables control of redundant transmission paths in a ring topology. MRP uses the special multicast MAC addresses: 01:15:4E:00:00:01 and 01:15:4E:00:00:02

7.4 Asynchronous communication connections

Overview of communication services

The CPU supports the following communication services:

Communication service	Functionality	Ethernet
PG communication	Commissioning, testing, diagnostics	Yes
HMI communication	Operator control and monitoring	Yes
S7 communication	Data exchange using configured connections	Yes
PROFINET IO	Data exchange between I/O controllers and I/O devices	Yes
Web server	Diagnostics, maintenance, and process data	Yes
SNMP (Page 265) ¹ (Simple Network Management Protocol)	Standard protocol for network diagnostics and parameterization	Yes
Open communication over TCP/IP	Data exchange over Industrial Ethernet with TCP/IP protocol (with Open user communication instructions)	Yes
Open communication over ISO on TCP	Data exchange over Industrial Ethernet with ISO on TCP protocol (with Open user communication instructions)	Yes
Open communication over UDP	Data exchange over Industrial Ethernet with UDP protocol (with Open user communication instructions)	Yes
Near Field Communication (NFC) (Page 315)	Data exchange between the PLC and a mobile phone	No

¹ The CPU supports SNMP V1 without TRAPs (alarm frames).

Available connections

The CPU supports a fixed number of maximum simultaneous asynchronous communication connections for PROFINET; you cannot change these values. You can configure the "Free available connections" to increase the number of any category as required by your application.

Some connection types have a fixed number of reserved resources (sometimes called guaranteed). This means that the CPU is guaranteed to support up to the number of reserved resources for the connection type. Additional connections beyond the number of reserved resources can be made for a connection type, but those connection resources must come from the "dynamic" resources pool.

The dynamic resources (sometimes called Free) are a collection of resources that can be used for any connection type. These resources are used by connections that do not have any reserved resources or by connections that have used up all of their reserved resources.

S7-1200 G2 CPUs have 10 reserved connection resources and 78 dynamic resources for a total of 88 connection resources.

Based upon the allocated connection resources, the following number of connections per CPU are available:

Type	Maximum guaranteed connections	Maximum dynamic connections	Total connections possible ²
Programming device (PG) communication	4	78 ¹	82
Human Machine Interface (HMI) communication	4	78 ¹	82
S7 communication	0	78 ¹	78
Open User communication	0	78 ¹	78
Web communication	2	78	80

¹ Adding CMs/CPs allows for 40 additional dynamic connections.

² Since the dynamic connections are shared, it is not possible to max out all connections simultaneously.

For an example, the CPU has four available PG connection resources. Depending on the current PG functions in use, the PG might actually use one, two, three, or four of its available connection resources. You can always use one PG.

NOTE

Web server connections: The CPU provides connections for multiple Web browsers. The number of browsers that the CPU can simultaneously support depends upon how many connections a given Web browser requests/utilizes and the number of dynamic connection resources available in the CPU.

NOTE

The Open user communication, S7 connection, HMI, programming device, and Web server communication connections can utilize multiple connection resources based upon the features currently being used.

7.5 Supported certificates

Secure communication services require certificates with certain security parameters.

You can create or select these certificates from the following areas in the TIA Portal "General" tab of the CPU "Properties" window:

- "Web server > Security": Use for the generation and assignment of Web server certificates.
- "Protection & Security > Connection mechanisms": Use for the generation or assignment of PLC communication or Secure PG/PC and HMI communication certificates.
- "Protection & Security > Certificate manager": Use for the generation or assignment of all types of certificates. The default setting for the creation of certificates is TLS certificates for Secure Open User Communication (Secure OUC), Syslog, and OPC UA.

For more information on generating and assigning certificates or certificate parameters, refer to the TIA Portal Information System.

7.6 PROFINET

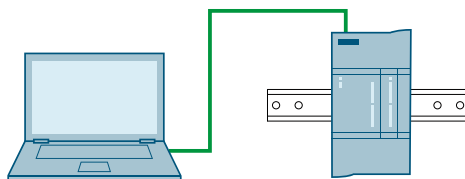
7.6.1 CPU communication

The S7-1200 G2 CPU can communicate with the following devices:

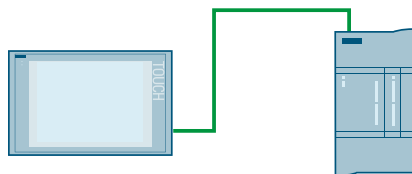
- Other CPUs
- Programming devices
- HMI devices
- Non-Siemens devices using standard TCP communications protocols

Example connections are as follows:

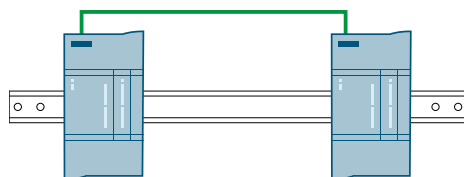
Programming device connected to the CPU ([Page 242](#))



HMI connected to the CPU ([Page 246](#))



A CPU connected to another CPU (Page 248)



NOTE

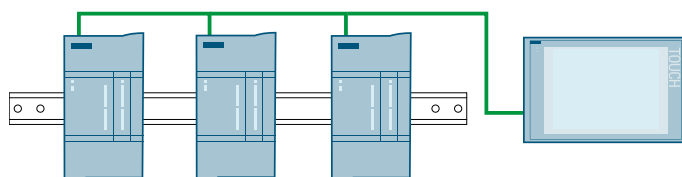
S7-1200 G2 CPUs do not support the IE/PB Link module.

Ethernet switching

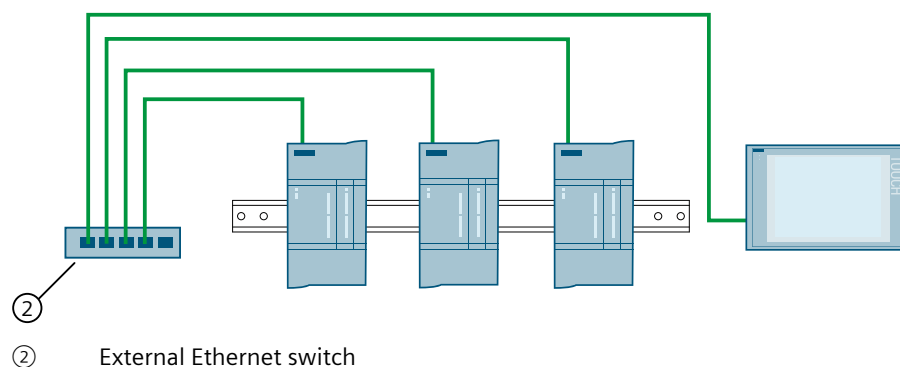
The S7-1200 G2 CPUs have a built-in 2-port Ethernet switch. You can use these built-in switches to create a network.

Example connections are as follows:

Multiple CPUs connected to an HMI device using the built-in 2-port Ethernet switch



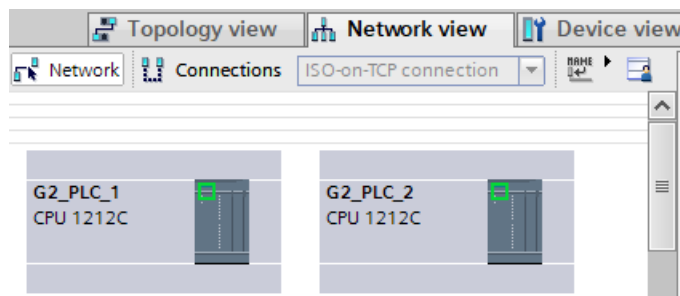
Multiple CPUs connected to an HMI device using an external ethernet switch



7.6.2 Creating a network connection

Use the "Network view" of Device configuration to create the network connections between the devices in your project.

1. Select "Network view" to display the devices to be connected.

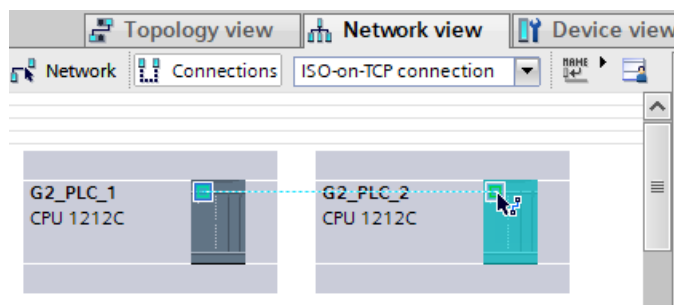


2. Select the "Connections" tab in the toolbar of Network view and choose your connection type from the dropdown menu.

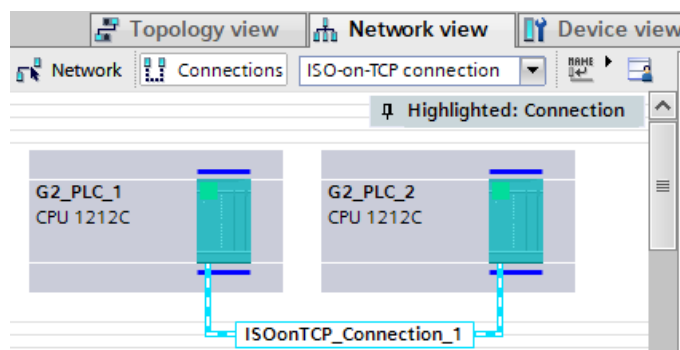
Note: the S7-1200 G2 supports the following connections:

- S7 connection ([Page 267](#))
- ISO-on-TCP connection ([Page 236](#))
- TCP connection ([Page 236](#))
- UDP connection ([Page 237](#))
- HMI connection ([Page 246](#)) (PLC to an HMI)

3. Select the port on one device and drag the connection to the port on the second device.



4. Release the mouse button to create the network connection.



After creating the network connection, use the "Properties" tab of the inspector window to configure the parameters of the network.

7.6.3 Configuring the Local/Partner connection path

A Local/Partner (remote) connection defines a logical assignment of two communication partners to establish communication services. A connection defines the following:

- Communication partners involved (one active, one passive)
- Type of connection (for example, a PLC, HMI, or device connection)
- Connection path

Communication partners execute the instructions to set up and establish the communication connection. You use instruction parameters to specify the active and passive communication end point partners. After the STEP 7 program sets up and establishes the connection, the CPU automatically maintains and monitors the connection.

If the connection is terminated (for example, due to a line break), the active partner attempts to re-establish the configured connection. You do not have to execute the communication instruction again.

For more information, see the following:

- "Connection configuration
(https://docs.tia.siemens.cloud/access?ft:originId=../10866368523/42307475211_enUS.htm&ft:clusterId/10866368523/42307475211.htm)"
- "Connection parameters
(https://docs.tia.siemens.cloud/access?ft:originId=../10866368523/13452671883_enUS.htm&ft:clusterId/10866368523/13452671883.htm)"

7.6.4 Locating the Ethernet (MAC) address on the CPU

In PROFINET networking, a Media Access Control address (MAC address) is an identifier assigned to the network interface by the manufacturer for identification. A MAC address usually encodes the manufacturer's registered identification number.

The standard (IEEE 802.3) format for printing MAC addresses in human-friendly form is six groups of two hexadecimal digits, separated by hyphens (-) or colons (:), in transmission order, (for example, 01-23-45-67-89-ab or 01:23:45:67:89:ab).

Each CPU is loaded at the factory with a permanent, unique MAC address. You cannot change the MAC address of a CPU.

The MAC address is printed on the front, upper-left corner of the CPU. Note that you have to lower the upper door to see the MAC address information.

The CPU interface is designated as X1, and initially has no IP address, only a factory-installed MAC address. PROFINET communication requires that all devices be assigned a unique IP address.

NOTE

Three sequential MAC addresses are assigned to the CPU:

- The lowest number, the number printed on the CPU, is for the X1 interface.
- The next higher number is for port P1R.
- The highest number is for port P2R.

The low-level protocols ([Page 258](#)) require the MAC addresses for P1R and P2R.

7.6.5 Assigning Internet Protocol (IP) addresses

7.6.5.1 Assigning IP addresses to programming and network devices

If the network interface of your programming device connects to a local area network (LAN) with multiple subnets, both the programming device and the CPU must be on the same subnet. You assign the subnet as a combination of the IP address and subnet mask for the device. See your local network administrator for help.

The Network ID of a Class C IP address is the first three octets of the IP address. The network ID of 211.154.184.16, for example, is 211.154.184. This network ID uniquely identifies your IP network. The subnet mask normally has a value of 255.255.255.0. Because your computer is on a plant LAN, however, the subnet mask might have various values, for example, 255.255.254.0, to set up unique subnets. The subnet mask, when combined with the device IP address in a logical AND operation, defines the boundaries of an IP subnet.

NOTE

You must assign unique IP addresses to all devices on your subnet.

WARNING

Unauthorized access to a CPU

Users with CPU full access or full access (incl. fail-safe) privileges have privileges to read and write PLC variables. Regardless of the access level for the CPU, Web server users can have privileges to modify PLC data and execute functions. Unauthorized access to the CPU can disrupt process operation.

Siemens recommends that you observe the following security practices:

- Enable Access control under "Protection & Security > Access control".
- Do not enable the "Anonymous" user.
- Use strong passwords, as defined in STEP 7.
- Use a secure Virtual Private Network (VPN) to connect to the S7-1200 G2 PLC from a location outside your protected network.
- Perform error-checking and range-checking on your variables in your program logic because Web server or users can change PLC variables to invalid values.

Disruption of process operations can result in death, severe personal injury, and/or property damage.

NOTE

A secondary network adapter card is useful when you do not want your CPU on your company LAN. During initial testing or commissioning tests, this arrangement is particularly useful.

Assigning or checking the IP address of your programming device

To assign or check your programming device's IP address, follow these steps:

1. Open the Control Panel.
2. Navigate to the "Network and Sharing Center".
3. Click "Change adapter settings" in the left column.
4. Right-click the network interface connected to your CPU.
5. Select "Properties" to open the properties dialog.
6. In the properties dialog, select the checkbox for "Internet Protocol Version 4 (TCP/IPv4)".
7. Click the "Properties" button.
8. Select "Obtain an IP address automatically" or to enter a static IP address select "Use the following IP address".

If you selected "Use the following IP address", set the IP address and subnet mask:

- Set the IP address to use the same Network ID and same subnet as the CPU. For example, if the CPU IP address is **192.168.0.1**, you could set the IP address to **192.168.0.200**.
- Select a subnet mask of 255.255.255.0.
- Leave the default gateway blank.

Consult your network administrator to help you set up a network configuration to allow you to connect to the S7-1200 G2 CPU.

7.6.5.2 Checking the IP address and MAC address of your network interface

To check the MAC and IP addresses of your network interface in STEP 7, follow these steps:

1. In the "Project tree", expand "Online access".
2. Right-click the required network interface, and select "Properties".
3. In the dialog, expand "Configurations", and select "Industrial Ethernet".

The window displays the MAC and IP addresses of the network interface.

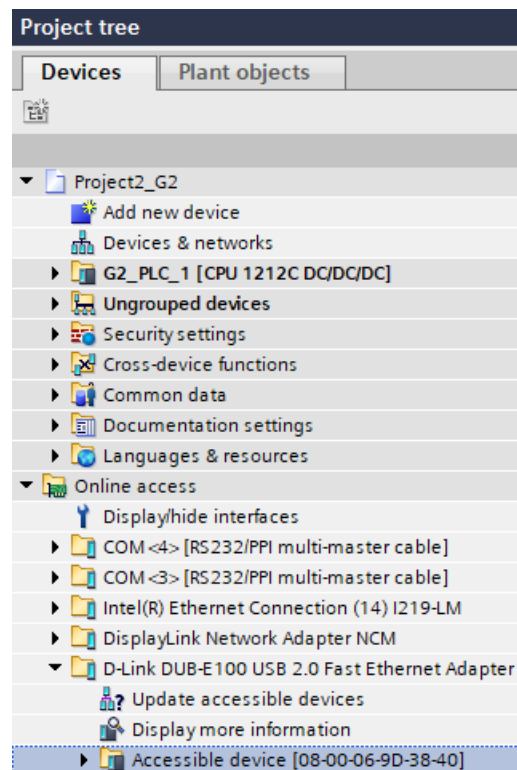
7.6.5.3 Assigning an IP address to an online CPU

You can assign an IP address to a network device online. This is particularly useful in an initial device configuration.

To verify that the CPU does not have a configured IP address, do the following:

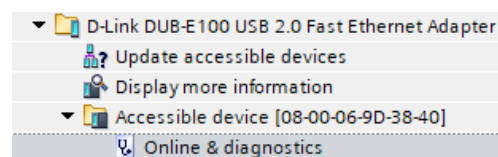
1. In the "Project tree", expand "Online access".
2. Expand the network in which the device is located.
3. Double-click "Update accessible devices".

If STEP 7 displays a MAC address instead of an IP address, then no IP address has been assigned.



To assign an IP address, follow these steps:

1. Expand the PLC for which you want to assign an IP address.
2. Double-click "Online & diagnostics".

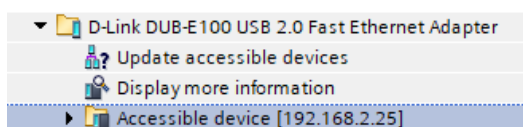


3. In the "Online & diagnostics" dialog, select "Functions > Assign IP address".

4. In the "IP address" field, enter your new IP address, and click "Assign IP address".



To verify that STEP 7 has assigned your new IP address to the CPU, double-click "Update accessible devices". It should now display the IP address that you configured.



7.6.5.4 Configuring an IP address for a CPU in your project

Configuring the PROFINET interface

In the Device configuration (Page 158) of the CPU, you can configure parameters for the PROFINET interface. Click the green PROFINET interface on the CPU and then select the "Properties" tab in the inspector window to display the PROFINET port.

Subnet and Subnet mask

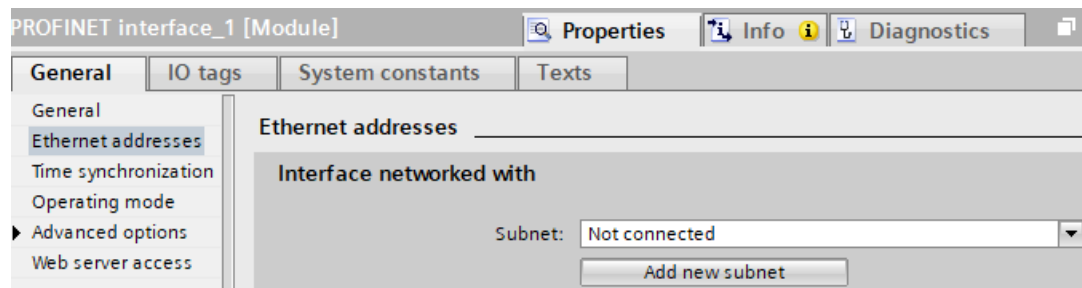
A subnet is a logical grouping of connected network devices. Nodes on a subnet tend to be located in close physical proximity to each other on a Local Area Network (LAN). A mask, known as the subnet mask or network mask, defines the boundaries of an IP subnet.

A subnet mask of 255.255.255.0 is suitable for a small local network. This means that all IP addresses on this network should have the same first three octets, and the various devices on this network are identified by the last octet (8-bit field). An example of this is to assign a subnet mask of 255.255.255.0 and an IP address of 192.168.2.0 through 192.168.2.255 to the devices on a small local network.

The only connection between different subnets is through a router. You must use an IP router if you use more than one subnet.

To set your subnet in your STEP 7 project, follow these steps:

1. In Device configuration, select the "Properties" Tab.
2. Under the "General" tab, select "Ethernet addresses".
3. In the "Interface networked with" section, click "Add new subnet" to create a new subnet. The default "Not connected" provides a local connection. You can choose a previously added subnet from the dropdown menu.



Internet Protocol (IP) address

Each device must also have an Internet Protocol (IP) address. This address allows the device to deliver data on a more complex, routed network. Each IP address is divided into four 8-bit octets and is expressed in a dotted, decimal format (for example, 211.154.184.16). The first part of the IP address is used for the Network ID, and the second part of the address is for the Host ID which is unique for each device on the network. An IP address of 192.168.x.y is a standard designation recognized as part of a private network that is not routed on the Internet.

In your STEP 7 project, you can configure how the IP address is set. In Device configuration, click the "Properties" Tab and select "Ethernet addresses". Choose one of the following options:

- Set IP address in the project
- IP address from DHCP (Dynamic HostConfiguration Protocol) server
- IP address is set directly at the device

Optionally, select "Use router" and enter the router's IP address if your network uses a router.

The screenshot shows the "Internet Protocol Version 4 (IPv4)" configuration window. It contains several sections for setting network parameters:

- Set IP address in the project:** This section is selected with a radio button. It includes fields for "IP address:" (192 . 168 . 0 . 2) and "Subnet mask:" (255 . 255 . 255 . 0).
- Use router:** This option is unchecked. It includes a "Router address:" field (0 . 0 . 0 . 0).
- IP address from DHCP server:** This option is selected with a radio button. It includes a "Mode:" dropdown menu (set to "Use MAC address as client ID"), a "Client ID:" text field, and a checked checkbox for "Client ID can be modified at runtime".
- IP address is set directly at the device:** This option is unselected with a radio button.

Table 7-4 Parameters for the IP address

Protocol	Parameter	Description
Set IP address in the project	IP address	Assigned IP address for the CPU
	Subnet mask	Assigned subnet mask
Use router		Click the checkbox to indicate the use of an IP router. Routers are the link between LANs. Using a router, a computer in a LAN can send messages to any other networks, which might have other LANs behind them. If the destination of the data is not within the LAN, the router forwards the data to another network or group of networks where it can be delivered to its destination. Routers rely on IP addresses to deliver and receive data packets.
	Router address	Assigned IP address for the router, if applicable
IP address from DHCP server	Mode	An external DHCP server provides the IP address (https://docs.tia.siemens.cloud/access?ft:originId=, /10866368523/139974759307_enUS.htm&ft:clusterId, /10866368523/139974759307.htm) based on either the MAC address of your network interface or an optional client ID. However, if the client ID is not configured, the server will not provide the MAC address as the identification.
	Client ID	
IP address is set directly at the device		Click the radio button set the IP address set directly at the device.

NOTE

The download operation sets all IP addresses for devices configured as "Set IP address in the project". If the CPU does not have a pre-configured IP address, download to the accessible device with the MAC address of your target device. If your CPU is connected to a router on a network, you must also enter the IP address of the router.

The "IP address is set directly at the device" radio button allows you to change the IP address through a tool such as the SIMATIC Automation Tool, Online & Diagnostics in the TIA Portal (Page 226), or by using the T_CONFIG instruction (Page 238) after the program is downloaded.

! WARNING**Downloading a hardware configuration with "IP address is set directly at the device"**

After downloading a hardware configuration with the "IP address is set directly at the device" option enabled, you cannot use communication functions to transition the CPU from RUN to STOP or from STOP to RUN until you set an IP address. User equipment continues to run under these conditions and can result in unexpected equipment and process operations.

Ensure that your CPU IP address(es) are set before using the CPU in an actual automation environment. This can be done by using STEP 7, the SIMATIC Automation Tool, or an attached HMI device in conjunction with the T_CONFIG instruction.

Unexpected equipment and process operations can cause death, severe personal injury, or property damage if proper precautions are not taken.

⚠ WARNING**Condition in which PROFINET network might stop**

Changing the IP address of a CPU online or from the STEP 7 program can create a condition where the PROFINET network might stop. If the CPU's IP address is changed to one outside the subnet, the PROFINET network loses communication, and all data exchange stops. User equipment might be configured to keep running under these conditions. Loss of PROFINET communication can result in unexpected machine or process operations.

If an IP address must be changed, ensure that the new IP address lies within the subnet.

Unexpected machine or process operations can cause death, severe personal injury, or property damage if proper precautions are not taken.

Configuring the PROFINET port

By default, the CPU configures port(s) of the PROFINET interface for autonegotiation, a feature that allows connected devices to automatically determine and configure the best possible parameters for communication. For autonegotiation to function properly, you must configure both stations to autonegotiate. If one station has a fixed configuration (for example, full-duplex at 100 Mbps) and the other station is set to autonegotiate, then autonegotiation fails, resulting in half-duplex operation.

To overcome this limitation of autonegotiation, the S7-1200 G2 provides an option to disable autonegotiation. When you disable autonegotiation, the S7-1200 G2 is automatically configured for full-duplex operation at 100 Mbps.

To set the transmission rate and duplex to a fixed value for each port, follow these steps:

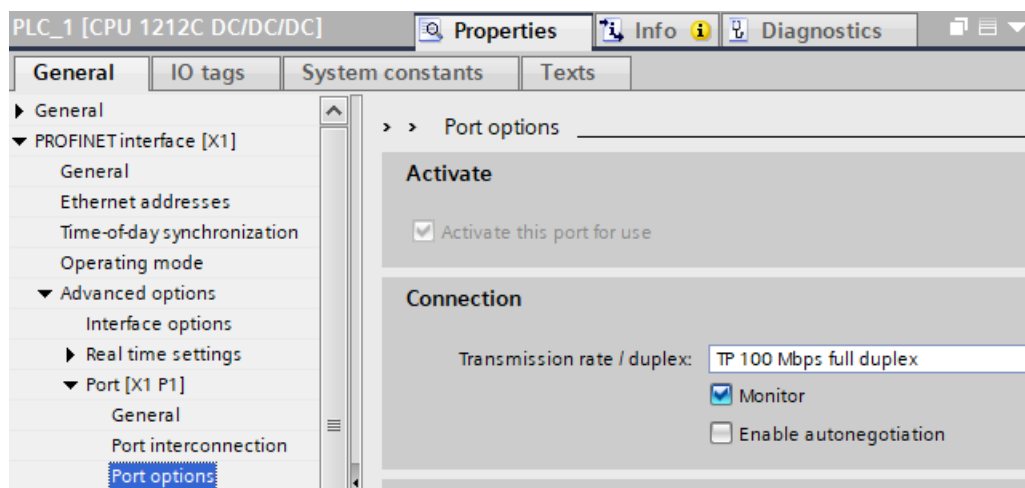
1. Select Advanced options and the port you need to configure. Then, select Port options.
2. In the Connection, Transmission rate / duplex field, select one of the following:
 - Automatic: The CPU and the peer device determine the port's transmission rate and duplex by autonegotiation.
 - TP 100 Mbps full-duplex: If you disable autonegotiation, the port operates at 100 Mbps full-duplex. If you enable autonegotiation, the port can operate at 100 Mbps full-duplex or another transmission rate / duplex that is autonegotiated between the CPU and the peer device. This places a message in the diagnostics buffer if "Monitor" is selected (see below).

You have the option to select the following parameters:

- Monitor: When you select this checkbox, the CPU places a message in the diagnostics buffer if any of the following occur at the port:
 - A link cannot be established
 - An established link fails
 - You select "TP 100 Mbps full-duplex" as the Transmission rate / duplex, and the CPU establishes a link using autonegotiation with the negotiated transmission rate not equal to 100 Mbps or the negotiated duplex equal to half-duplex.
- Enable autonegotiation: Once you set the Transmission rate / duplex field to full-duplex at 100 Mbps, you can then disable autonegotiation. Deselect the "Enable autonegotiation" checkbox to disable autonegotiation.

NOTE

If you disable autonegotiation, the CPU and the peer device do not negotiate the port's transmission rate and duplex.

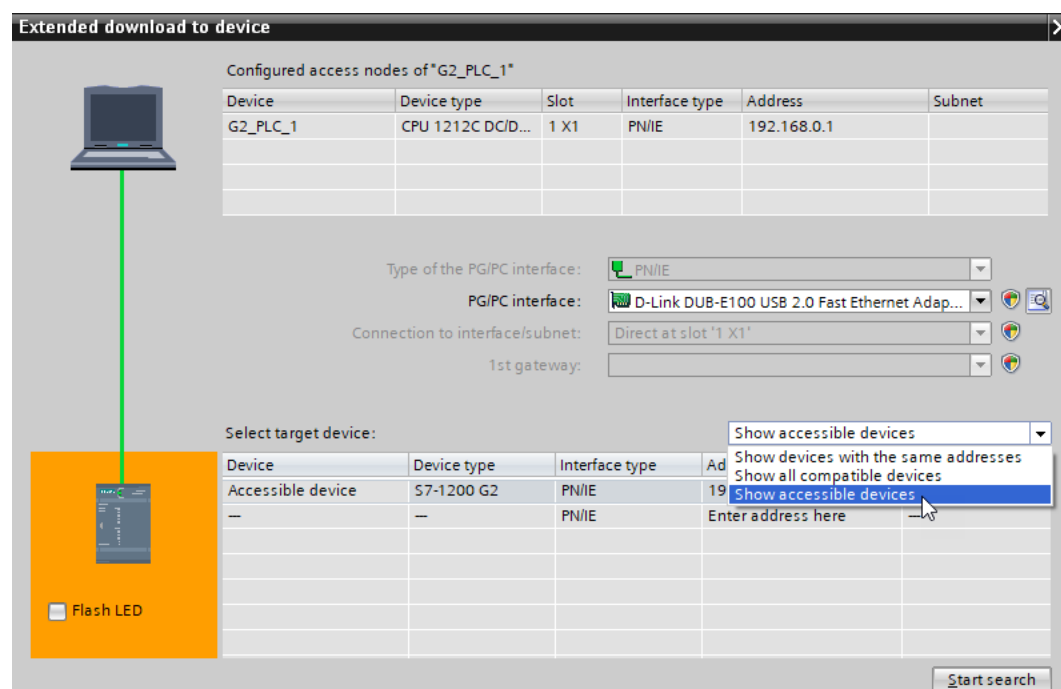


7.6.6 Testing the PROFINET network

After completing the configuration, download the project (Page 173) to the CPU.

Using the "Extended download to device" dialog to test for connected network devices

The S7-1200 G2 CPU "Download to device" function and its "Extended download to device" dialog show all accessible network devices and whether unique IP addresses have been assigned to all devices. To display all accessible and available devices with their assigned MAC or IP addresses, select "Show accessible devices" from the "Select target device" dropdown menu.



If the required network device is not in this list, communications to that device have been interrupted. The device and network must be investigated for hardware and/or configuration errors.

7.6.7 PROFINET device startup time, naming, and address assignment

PROFINET IO can extend the startup time for your system (Configuration time). More devices and slow devices impact the amount of time it takes to switch to RUN.

On your PROFINET network, you can have a maximum of 31 PROFINET IO devices, reducing to 30 devices if the CPU is an I-Device and 29 if the CPU is a shared I-Device.

All PROFINET devices must have a Device name and an IP Address.

Each station (or IO Device) starts up independently on startup, and this affects the overall CPU startup time. If you set the "Configuration time" too low, there might not be a sufficient overall CPU startup time for all stations to complete startup. If this situation occurs, false station errors will result.

The default Configuration time is 60,000 ms (1 minute). You can configure this in CPU Properties > Startup > Configuration time.

PROFINET address assignment at system startup

The controller broadcasts the names of the devices to the network, and the devices respond with their MAC addresses. The controller then assigns an IP address to the device using the PROFINET DCP protocol:

- If the MAC address has a configured IP address, then the station performs startup.
- If the MAC address does not have a configured IP address, STEP 7 assigns the address that is configured in the project, and the station then performs startup.

If there is a problem with this process, a station error occurs and no startup takes place. This situation causes the configurable time-out value to be exceeded.

7.6.8 Configuring Network Time Protocol (NTP) synchronization

The Network Time Protocol (NTP) is widely used to synchronize the clocks of computer systems to Internet time servers. In NTP mode, the CPU sends time-of-day queries at regular intervals (in the client mode) to the NTP server in the subnet (LAN). Based on the replies from the server, the NTP determines the most reliable and most accurate time and synchronizes the time of day on the querying module.

WARNING

Risk of network attacks through Network Time Protocol (NTP) synchronization

If an attacker can access your networks through Network Time Protocol (NTP) synchronization, the attacker can possibly disrupt control of your process by shifting the CPU system time.

The S7-1200 G2 CPU disables the NTP client feature by default. When you enable the NTP feature, then only the IP addresses that you configure can act as NTP servers. You must configure the NTP feature to allow CPU system time corrections from remote servers.

The S7-1200 G2 CPU supports "time of day" interrupts and clock instructions that depend upon accurate CPU system time. If you configure NTP and accept time synchronization from a server, you must ensure that the server is a trusted source. Failure to do so can cause a security breach that allows an unknown user to disrupt control of your process by shifting the CPU system time.

For security information and recommendations, see the "Operational Guidelines (<https://www.siemens.com/global/en/products/services/cert/news/operational-guidelines-for-industrial-security.html>)" white paper on the Siemens Industrial Cybersecurity Web site. Disruptions to process control can cause death, severe injury, or property damage.

The advantage of NTP mode is that it allows the time to be synchronized (https://docs.tia.siemens.cloud/access?ft:originId=/.52541677963/31476189579_enUS.htm&ft:clusterId/.52541677963/31476189579_enUS.htm) across subnets.

7.6.9 Open user communication

7.6.9.1 Protocols

The integrated PROFINET interface of the CPU supports multiple communications standards over an Ethernet network:

- Transport Control Protocol (TCP) ([Page 236](#))
- ISO on TCP ([Page 236](#))
- User Datagram Protocol (UDP) ([Page 237](#))

Table 7-5 Protocols and communication instructions for each

Protocol	Usage examples	Entering data in the receive area	Communication instructions	Addressing type
TCP (Page 236)	CPU-to-CPU communication Transport of frames	Ad hoc mode (Page 237)	Only TRCV_C and TRCV	Assigns port numbers to the Local (active) and Partner (passive) devices
		Data reception with specified length	TSEND_C, TRCV_C, TCON, TCONSettings, TDISCON, TSEND, TRCV, T_RESET, and T_DIAG	

Protocol	Usage examples	Entering data in the receive area	Communication instructions	Addressing type
ISO on TCP (Page 236)	CPU-to-CPU communication Message fragmentation and re-assembly	Ad hoc mode	Only TRCV_C and TRCV	Assigns TSAPs to the Local (active) and Partner (passive) devices
		Protocol-controlled	TSEND_C, TRCV_C, TCON, TCONSettings, TDISCON, TSEND, TRCV, T_RESET, and T_DIAG	
UDP (Page 237)	CPU-to-CPU communication STEP 7 program communications	User Datagram Protocol	TUSEND and TURCV	Assigns port numbers to the Local (active) and Partner (passive) devices, but is not a dedicated connection

7.6.9.2 TCP, ISO on TCP, and UDP

TCP

Transport Control Protocol (TCP) is a standard protocol described by RFC 793: Transmission Control Protocol (<https://www.rfc-editor.org/info/rfc793>). The primary purpose of TCP is to provide reliable connection service between pairs of processes. Most of the user application protocols, such as TELNET and FTP, commonly use TCP. This protocol offers the following features and capabilities:

- Offers an efficient communications protocol that is closely tied to the hardware
- Allows for the handling of data amounts up to 64 KB.
- Provides extensive facilities for applications, notably error recovery, flow control, and reliability
- Operates as a connection-oriented protocol
- Offers flexibly for integration with third-party systems that exclusively support TCP
- Provides routing capabilities
- Supports only static data lengths
- Acknowledges messages
- Addresses applications using port numbers
- Requires programming effort for data management due to the SEND / RECEIVE programming interface

ISO on TCP

International Organization for Standardization on Transport Control Protocol, commonly known as "ISO on TCP", is described by RFC 1006 (<https://www.rfc-editor.org/info/rfc1006>) as a mechanism that enables ISO applications to be ported to the TCP/IP network. This protocol has the following features and capabilities:

- Offers an efficient communications protocol that is closely tied to the hardware
- Allows for the handling of medium-sized to large data amounts (up to 64 KB)
- Provides routing capabilities; can be used in WAN
- Supports dynamic data lengths
- Requires programming effort for data management due to the SEND / RECEIVE programming interface

In contrast to TCP, the messages feature an end-of-data identification and are message-oriented.

Using Transport Service Access Points (TSAPs), TCP protocol allows multiple connections to a single IP address (up to 64K connections). With RFC 1006, TSAPs uniquely identify these communication end point connections to an IP address.

UDP

UDP

(https://docs.tia.siemens.cloud/access?ft:originId=../10866368523/25643073419_enUS.htm&ft:clusterId../10866368523/25643073419.htm) is a standard protocol described by RFC 768: User Datagram Protocol (<https://www.rfc-editor.org/info/rfc768>). UDP is a simpler transport control protocol than TCP that provides a mechanism for one application to send a datagram to another; however, delivery of data is not guaranteed. UDP has the following features and capabilities:

- Offers a quick communications protocol
- Allows for the handling of small-sized to medium data amounts (up to 2048 bytes)
- Provides a thin layer that yields low overheads
- Offers flexibly for integration with many third-party systems
- Provides routing capabilities
- Uses port numbers to direct the datagrams
- Requires the application to take responsibility for error recovery and security as messages are unacknowledged
- Requires programming effort for data management due to the SEND / RECEIVE programming interface

UDP supports broadcast communication. To use broadcast, you must configure the IP address portion of the ADDR configuration. For example: A CPU with an IP address of 192.168.2.10 and subnet mask of 255.255.255.0 would use a broadcast address of 192.168.2.255.

7.6.9.3 Ad hoc mode

Typically, TCP and ISO on TCP receive data packets of a specified length, ranging from 1 to 8192 bytes. However, the TRCV C

(https://docs.tia.siemens.cloud/access?ft:originId=../18560165643/19135463947_enUS.htm&ft:clusterId../18560165643/19135463947.htm) and TRCV

(https://docs.tia.siemens.cloud/access?ft:originId=../18560165643/19142302219_enUS.htm&ft:clusterId../18560165643/19142302219.htm) communication instructions also

provide an "ad hoc" communications mode that can receive data packets of a variable length from 1 to 1460 bytes.

7.6.9.4 Instructions

Open user communication instructions (https://docs.tia.siemens.cloud/access?ft:originId=./10866368523/13367222283_enUS.htm&ft:clusterId./10866368523/13367222283.htm) provide for communication using various network protocols and include the following folder groups:

Communication	
Name	Description
▶ S7 communication	
▼ Open user communication	
▶ TSEND_C	Establishing a connection and sending data
▶ TRCV_C	Establishing a connection and receiving data
▶ TMAIL_C	Send e-mail
▶ CommConfig	Read and modify communication parameters
▼ Others	
▶ TCONSettings	Prepare and change communication connection
▶ TCON	Establish communication connection
▶ TDISCON	Terminate communication connection
▶ TSEND	Send data via communication connection
▶ TRCV	Receive data via communication connection
▶ TUSEND	Send data via Ethernet (UDP)
▶ TURCV	Receive data via Ethernet (UDP)
▶ T_RESET	Resetting the connection
▶ T_DIAG	Checking the connection
▶ T_CONFIG	Configure interface

NOTE

Choosing an instruction by PLC family

If the TIA Portal Information System presents an instruction differently within the tooltips or table of contents based on PLC family, follow the S7-1500 option for the instruction topic.

7.6.9.5 Connection IDs for the Open user communication instructions

Create an instance DB to configure the communications channel (or connection) between the devices by inserting the TSEND_C, TRCV_C or TCON instructions into STEP 7. To configure the parameters for the connection, utilize the Properties of the instruction. One of these parameters is the connection ID, which must be unique for the CPU. Ensure that each connection you create has a different DB and connection ID. Also, note the following:

- Both the local CPU and the partner CPU can use the same connection ID number for the same connection, but the connection ID numbers are not required to match. The connection ID number is relevant only for the Open user communication instructions within the user program of the individual CPU.
- You can use any number in the range of 1 to 4095 for the connection ID of the CPU. However, configuring the connection IDs sequentially from "1" provides an easy method for tracking the number of connections in use for a specific CPU. Alternatively, you can use the TCONSettings instruction to request a connection ID from the CPU.

NOTE

Each TSEND_C, TRCV_C, or TCON instruction in STEP 7 creates a new connection. It is important to use the correct connection ID for each connection.

For more information, see the following topics in the Open User Communication chapter of the TIA Portal Information System:

- TCON: Establish communication connection (S7-1200, S7-1500)
(https://docs.tia.siemens.cloud/access?ft:originId=../18560165643/46790960779_enUS.htm&ft:clusterId/18560165643/46790960779.htm)
- TSEND_C: Establishing a connection and sending data
(https://docs.tia.siemens.cloud/access?ft:originId=../18560165643/41150802699_enUS.htm&ft:clusterId/18560165643/41150802699.htm)
- TRCV_C: Establishing a connection and receiving data
(https://docs.tia.siemens.cloud/access?ft:originId=../18560165643/41150876811_enUS.htm&ft:clusterId/18560165643/41150876811.htm)

7.6.9.6 Parameters for the OUC connection

The TSEND_C, TRCV_C, and TCON instructions require connection-related parameters (https://docs.tia.siemens.cloud/access?ft:originId=../10866368523/13452671883_enUS.htm&ft:clusterId/10866368523/13452671883.htm) to connect to the partner device. The TCON_Param structure assigns these parameters for the TCP, ISO-on-TCP, and UDP protocols. Use the "Configuration" tab of the "Properties" of the instruction to specify these parameters. If the "Configuration" tab is not accessible, provide the TCON_Param structure in the instruction parameters.

NOTE

If you specify the address of a device as an FQDN via the connection types of TCON_QDN or TCON_QDN_SEC, you need to configure a DNS server ([Page 240](#)).

NOTE

Connection types of TCON_QDN_SEC and TCON_IP_V4_SEC use TLS for security (Page 240).

7.6.9.7 Transport Layer Security (TLS)

TLS is Transport Layer Security in the application layer of data communications. TLS increases security and privacy in communication between the S7-1200 G2 CPU and other devices.

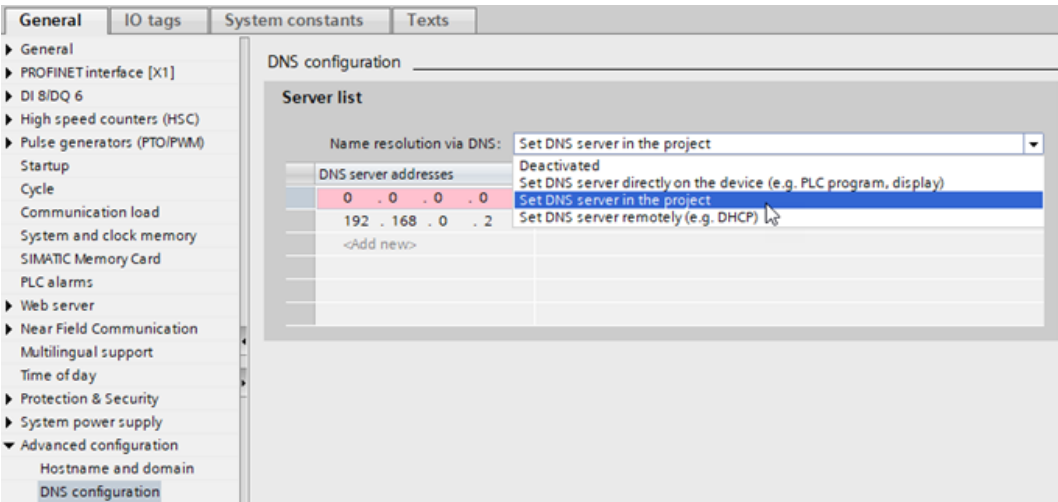
7.6.9.8 Configuring DNS

A DNS server might be required when the module itself, a communications partner, or for example an FTP server should be reachable via the host name (FQDN). If you specify the address of a connection partner as FQDN, configure a DNS server. In this case, the IP address of the connection partner is obtained via the configured DNS server.

To use DNS, you must have at least one DNS server in your network, and you must configure at least one DNS server for the S7-1200 G2 CPU.

To configure a DNS server, follow these steps:

1. From the Device view for your S7-1200 G2 CPU, navigate to "Properties > General".
2. Navigate to "Advanced configuration > DNS configuration" to display the configuration pane.
3. Select "Set DNS servers in the project" in the dropdown menu.



4. In the Server list table, click "<Add new>" and enter the IP address of your DNS server.

7.6.9.9 Configuring an OUC connection in the TIA Portal

For complete information on configuring an Open User Communication connection in STEP 7, see the following topics and chapters under "Using Open User Communication" in the TIA Portal Information System:

- Basics of Open User Communication
(https://docs.tia.siemens.cloud/access?ft:originId=../10866368523/1336722283_enUS.htm&ft:clusterId/10866368523/1336722283.htm)
- Connection configuration
(https://docs.tia.siemens.cloud/access?ft:originId=../10866368523/42307475211_enUS.htm&ft:clusterId/10866368523/42307475211.htm)
- Connection parameters
(https://docs.tia.siemens.cloud/access?ft:originId=../10866368523/13452671883_enUS.htm&ft:clusterId/10866368523/13452671883.htm)

7.6.9.10 Common parameters for instructions

REQ input parameter

Many of the OUC instructions use the REQ input to initiate the operation on a low to high transition. The REQ input must be high (TRUE) for one execution of an instruction, but the REQ input can remain TRUE for as long as you choose. The instruction does not initiate another operation until it has been executed with the REQ input FALSE so that the instruction can reset the history state of the REQ input. This is required so that the instruction can detect the low to high transition to initiate the next operation.

When you place one of these instructions in your program, STEP 7 prompts you to identify the instance DB. Use a unique DB for each instruction call. This ensures that each instruction properly handles inputs such as REQ.

ID input parameter

The ID parameter is a reference to the "Local ID (hex)" on the "Network view" of "Devices and networks" in STEP 7 and is the ID of the network that you want to use for this communication block. The ID must be identical to the associated parameter ID in the local connection description.

DONE, NDR, BUSY, ERROR, and STATUS output parameters

The following parameters are common to the OUC instructions and provide outputs describing the completion status:

Table 7-6 Open User Communication instruction output parameters

Parameter	Data type	Default	Description
DONE	Bool	FALSE	Is set TRUE for one execution to indicate that the last request completed without errors; otherwise, FALSE.
NDR	Bool	FALSE	Is set TRUE for one execution to indicate that the requested action has completed without error and new data has been received; otherwise, FALSE.

Parameter	Data type	Default	Description
BUSY	Bool	FALSE	Is set TRUE when active to indicate that: - The job is not yet complete. - A new job cannot be triggered. Is set FALSE when job is complete.
ERROR	Bool	FALSE	Is set TRUE for one execution to indicate that the last request completed with errors, with the applicable error code in STATUS; otherwise, FALSE.
STATUS	Word	0	Is set to a status value as follows: - If the DONE or NDR bit is set, then STATUS is set to 0 or to an informational code. - If the ERROR bit is set, then STATUS is set to an error code. - If none of the above bits are set, then the instruction returns status results that describe the current state of the function. STATUS retains its value for the duration of the execution of the function.

NOTE

Note that DONE, NDR, and ERROR are set for one execution only.

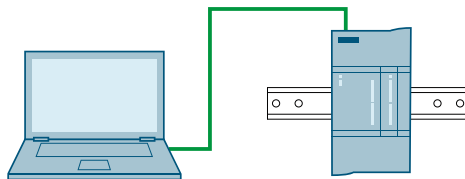
7.6.9.11 Restricted TSAPs or port numbers for passive ISO and TCP communication

If you use the TCON instruction to set up and establish a passive communications connection, do not use the following restricted port addresses:

- ISO TSAP (passive):
 - 01.00, 01.01, 02.00, 02.01, 03.00, 03.01
 - 10.00, 10.01, 11.00, 11.01, ... BF.00, BF.01
- TCP port (passive) and UDP port (passive):
 - 20, 21, 25, 80, 102, 443, 5001, 34962, 34963, 34964, 49152 to 65535

7.6.10 Communication with a programming device

A CPU can communicate with a STEP 7 programming device on a network.

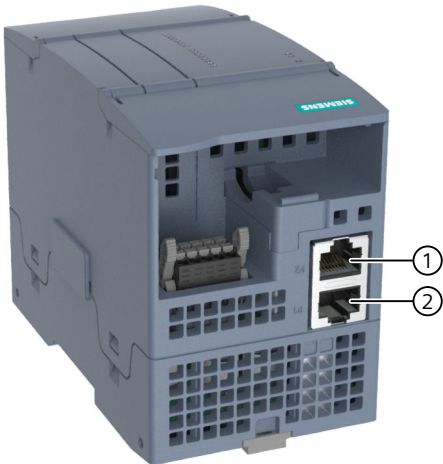


7.6.10.1 Establishing the hardware communications connection

PROFINET interfaces establish the physical connections between a programming device and a CPU. Since Auto-Cross-Over functionality is built into the CPU, either a standard or crossover Ethernet cable can be used for the interface. An Ethernet switch is not required to connect a programming device directly to a CPU.

Follow the steps below to create the hardware connection between a programming device and a CPU:

- 1. Install the CPU (Page 71).
- 2. Plug the Ethernet cable into one of the two PROFINET ports located on the top left of the CPU.
- 3. Connect the Ethernet cable to the programming device.



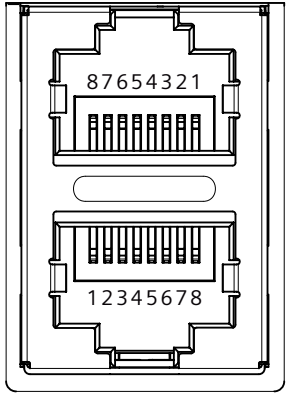
- ① X1P2
- ② X1P1

PROFINET interface X1 port pinouts

S7-1200 G2 CPUs connect to the PROFINET network using standard female RJ45 jacks. All S7-1200 G2 CPUs have dual-ports, but one interface. The connector pinout is the same for all CPUs.

The dual-ports of S7-1200 G2 CPUs have a standard Ethernet MDI-X pin configuration as follows:

Pin	Signal name	Description	RJ45 female jack pinout
1	TD+	Transmit data	
2	TD-		
3	RD+	Receive data	
4	GND	Ground	
5	GND		

Pin	Signal name	Description	RJ45 female jack pinout
6	RD-	Receive data	 X1P1 X1P2
7	GND	Ground	
8	GND		

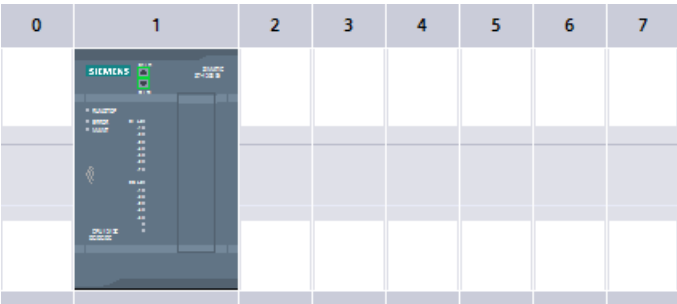
NOTE

All S7-1200 G2 CPUs are dual-port CPUs with no crossover between pins. There is an internal Ethernet switch in the units: The TD+/- and RD+/- pairs are not crossed over internally.

7.6.10.2 **Configuring the devices**

If you have already created a project with a CPU, open your project in STEP 7.

If not, create a project and insert a CPU (Page 159) into the rack.



Autonegotiation

If the port's configuration enables autonegotiation, the S7-1200 G2 CPU automatically detects the cable type and swaps the transmit/receive lines, if needed. If the port's configuration disables autonegotiation, the CPU also disables this automatic swap. You configure a port's autonegotiation setting (Page 227) in the TIA Portal's port options dialog. This is a port-specific advanced option for the PROFINET interface (X1) of the CPU's properties.

7.6.10.3 Testing the PROFINET network

After completing the configuration, download the project to the CPU. The download operation sets all IP addresses for devices configured as "Set IP address in the project".

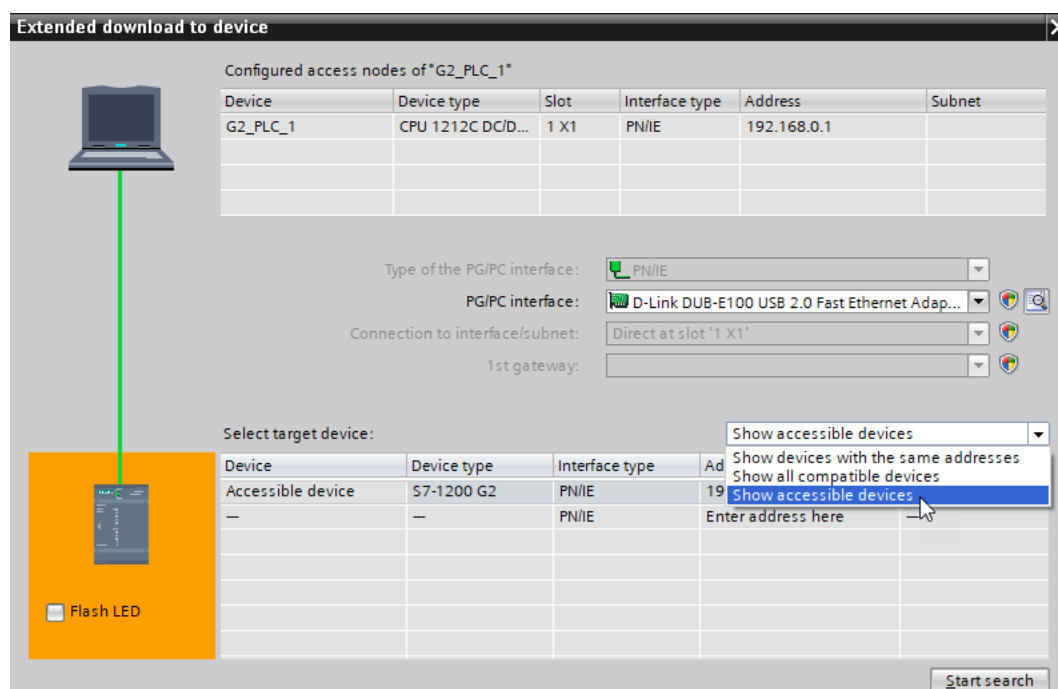
Assigning an IP address to an online CPU

The CPU does not have a pre-configured IP address. You must manually assign an IP address for the CPU in one of the following ways:

- Assign an IP address to an online CPU (Page 226).
- Assign IP address for a CPU in your project (Page 227). You must configure the IP address, save the configuration, and download it to the CPU.

Using the "Extended download to device" dialog to test for connected network devices

The CPU "Download to device" function and its "Extended download to device" dialog can show all accessible network devices and whether or not unique IP addresses have been assigned to all devices. To display all accessible and available devices with their assigned MAC or IP addresses, select "Show all accessible devices" from the dropdown menu.



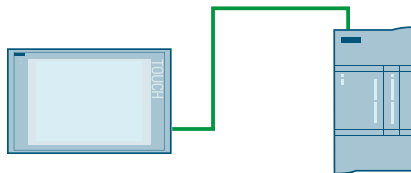
If the required network device is not in this list, communications to that device have been interrupted for some reason. Check the device and network for hardware or configuration errors.

7.6.10.4 Assigning Internet Protocol (IP) addresses

In a PROFINET network, each device must have an Internet Protocol (IP) address. This address allows the device to deliver data on a more complex, routed network:

- If you have programming or other network devices that use a network interface connected to your plant LAN or an Ethernet-to-USB adapter connected to an isolated network, you must assign IP addresses to them. Refer to "Assigning IP addresses to programming and network devices" (Page 224) for more information.
- You can also assign an IP address to a CPU or network device online (Page 226). This is particularly useful in an initial device configuration.
- After you have configured your CPU or network device in your project, you can configure parameters for the PROFINET interface to include its IP address. Refer to "Configuring an IP address for a CPU in your project" (Page 227) for more information.

The S7-1200 G2 CPU supports PROFINET communications connections to HMIs.



Consider the following requirements when setting up communications between CPUs and HMIs:

Configuration/Setup:

- The PROFINET port of the CPU must be configured to connect with the HMI.
- The HMI must be setup and configured.
- The HMI configuration information is part of the CPU project and can be configured and downloaded from within the project.
- The HMI driver must be selected from the Device wizard. The S7-1200 G2 CPU uses the "SIMATIC S7-1500" driver to communicate with Basic or Comfort HMIs, and the "SIMATIC S7-1200/1500" driver to communicate with Unified panels.

NOTE

All S7-1200 G2 CPUs feature one PROFINET interface equipped with two ports that operate as an Ethernet switch.

Configuring communication between the HMI and a CPU

To configure communication between the HMI and a CPU, do the following:

1. Establish the hardware communications connection (Page 243). A PROFINET interface establishes the physical connection between an HMI and a CPU. Since Auto-Cross-Over functionality is built into the CPU, you can use either a standard or crossover Ethernet cable for the interface. An Ethernet switch is not required to connect an HMI and a CPU.
2. Configure the device (Page 244).
3. Configure the logical network connections between an HMI and a CPU (Page 222).
4. Configure an IP address in your project (Page 227). You must configure IP addresses for the HMI and the CPU.
5. Test the PROFINET network (Page 245). You must download the configuration for each CPU and HMI device.

Supported HMI connection mechanisms

You can configure your HMI communication preferences in the "Device configuration" for your CPU under "Protection & Security > Connection mechanisms". The S7-1200 G2 supports the following HMI connection mechanisms based on panel type:

Panel type	S7-1200 G2 supported HMI connection mechanisms
Basic Panel	GET/PUT (Page 267)
	Secure PG/PC and HMI Communication
Comfort Panel	GET/PUT
	Secure PG/PC and HMI Communication
Unified Panel	GET/PUT
	Secure PG/PC and HMI Communication
	Standard Modbus TCP/IP (Page 309)

NOTE

Secure PG/PC and HMI Communication requires an HMI device image of V17 or later.

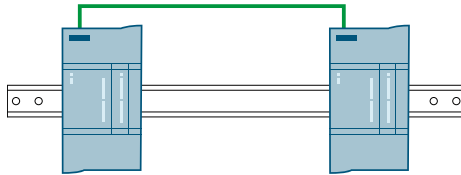
Supported HMI tags and subscriptions

The CPU supports 2000 tags for up to 250 HMI subscriptions. For further details on HMI connection resources and connection optimization, see the "Connection resources and connection optimization for HMI operator panels with S7-Controllers (<https://support.industry.siemens.com/cs/pl/en/view/109479986>)" FAQ.

See also[Supported certificates \(Page 220\)](#)**7.6.11 PLC-to-PLC communication**

A CPU can communicate with another CPU on a network.

One way to configure two CPUs to communicate with each other is by using the TSEND_C and TRCV_C instructions.



Consider the following when setting up communications between two CPUs:

- Configuration/Setup
- Supported functions: Reading/Writing data to a peer CPU
- No Ethernet switch is required for one-to-one communications; an Ethernet switch is required for more than two devices in a network unless the devices have a built in switch.

Configuring communication between two CPUs

To configure communication between two CPUs, follow these steps:

1. Establish the hardware communications connection [\(Page 243\)](#). A PROFINET interface establishes the physical connection between two CPUs. Since Auto-Cross-Over functionality is built into the CPU, you can use either a standard or crossover Ethernet cable for the interface. An Ethernet switch is not required to connect the two CPUs.
2. Configure the devices [\(Page 244\)](#). You must configure two CPUs in your project.
3. Configure the logical network connections between two CPUs [\(Page 222\)](#).
4. Configure an IP address in your project [\(Page 227\)](#). You must configure IP addresses for two CPUs (for example, PLC_1 and PLC_2).
5. Configure transmit (send) and receive parameters [\(Page 249\)](#). You must configure TSEND_C and TRCV_C instructions in both CPUs to enable communications between them.
6. Test the PROFINET network [\(Page 245\)](#). You must download the configuration for each CPU.

7.6.11.1 Configuring connection parameters

Configuring connection parameters

To specify the connection parameters, select any part of the instruction and do the following:

1. In the inspector window of STEP 7, select the "Properties" tab
2. Select the "Configuration" tab at right.
3. Select "Connection parameter".

Refer to "Configuring the Local/Partner connection path (Page 223)" for more information on each parameter.

Defining TSAPs (Transport Service Access Points) or Ports

If you configure a communication connection in your STEP 7 program, STEP 7 automatically assigns the TSAP

(https://docs.tia.siemens.cloud/access?ft:originId=../10866368523/13575570443_enUS.htm&ft:clusterId/10866368523/13575570443.htm).

If you are using TBlocks, you can edit the TSAP fields in the "Address Details" section of the Connection parameters dialog or directly in the connection parameter Data block .

7.6.11.2 Configuring transmit (send) and receive parameters

Communication blocks (for example, TSEND_C and TRCV_C) are used to establish a connection between two CPUs. Before the CPUs can engage in PROFINET communications, you must configure parameters for transmitting (or sending) messages and receiving messages.

For more information on Configuring the TSEND_C and TRCV_C instructions, see the following topics:

- TSEND_C: Establishing a connection and sending data
(https://docs.tia.siemens.cloud/access?ft:originId=../18560165643/41150802699_enUS.htm&ft:clusterId/18560165643/41150802699.htm)
- TRCV_C: Establishing a connection and receiving data
(https://docs.tia.siemens.cloud/access?ft:originId=../18560165643/41150876811_enUS.htm&ft:clusterId/18560165643/41150876811.htm)

7.6.12 Configuring a CPU and PROFINET IO device

7.6.12.1 Adding a PROFINET IO device

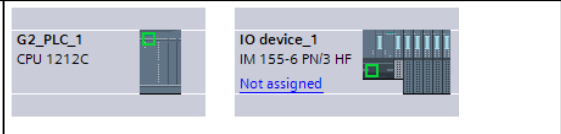
CPU-to-PROFINET IO device communication allows for data transmission and reception with specified length.

To add PROFINET IO devices in your STEP 7 program, follow these steps:

- 1. From the "Project tree", double click to select "Device configuration" for your CPU.
- 2. In the center window, select the "Network view" tab.
- 3. From the "Hardware catalog" pane at right, select the PROFINET IO device (sorted by part number).
- 4. Drag and drop the selected IO device into the "Network view" inspector window.

For example, expand the following containers in the hardware catalog to add an ET 200SP IO device: Distributed I/O, ET 200SP, Interface modules, and PROFINET. You can then select the interface module from the list of ET 200SP devices and add the ET 200SP IO device.

Table 7-7 Adding an ET 200SP IO device to the device configuration

Insert the IO device	Result
	

You can now connect the PROFINET IO device to the CPU:

- 1. Right-click the "Not assigned" link on the device and select "Assign new IO controller" from the context menu to display the "Select IO controller" dialog.
- 2. Select your CPU (in this example, "S7-1200 G2") from the list of IO controllers in the project.
- 3. Click "OK" to create the network connection.

You can also go to the "Devices and networks" window and use the "Network view" to create the network connections between the devices in your project:

- 1. To create a PROFINET connection, click the green (PROFINET) box on the first device, and drag a line to the PROFINET box on the second device.
- 2. Release the mouse button to configure the PROFINET connection.

Refer to "Device Configuration: Configuring the CPU for communication (Page 173)" for more information.

7.6.12.2 Assigning CPUs and device name

Network connections between the devices also assign the PROFINET IO device to the CPU, which is required for that CPU to control the device. To change this assignment, click the PLC name shown on the PROFINET IO device. Use the dialog box to disconnect the PROFINET IO device from the current CPU and reassign it to another CPU. Alternatively, you can leave the PROFINET IO device unassigned.

To connect with the CPU, you must assign a name to the devices on your PROFINET network (https://docs.tia.siemens.cloud/access?ft:originId=./19260980235/20299041291_enUS.htm&ft:clusterId./19260980235/20299041291.htm). If you have not assigned a name to the devices, or if you need to change a device's name, use the "Network view" option. Select the PROFINET IO device and right-click to choose "Assign device name".

NOTE

You must assign the same name to each PROFINET IO device in both the STEP 7 project and the PROFINET network.

You can use one of the following tools to assign the device name in the PROFINET network:

- STEP 7 "Online & diagnostics" tool
- PRONETA commissioning, configuration, and diagnostics tool
- SIMATIC Automation Tool

If a name is missing or does not match in either location, the PROFINET IO data exchange mode will not run.

7.6.12.3 Assigning Internet Protocol (IP) addresses

In a PROFINET network, each device must have an Internet Protocol (IP) address. Note the following:

- If you have programming or other network devices that use an onboard adapter interface connected to your plant LAN or an Ethernet-to-USB adapter card connected to an isolated network, you must assign IP addresses to them. Refer to "Assigning IP addresses to programming and network devices" ([Page 224](#)) for more information.
- You can also assign an IP address to a CPU or network device online. This is particularly useful in an initial device configuration. Refer to "Assigning an IP address to a CPU online" ([Page 226](#)) for more information.
- After you have configured your CPU or network device in your project, you can configure parameters for the PROFINET interface to include its IP address. Refer to "Configuring an IP address for a CPU in your project" ([Page 227](#)) for more information.

7.6.12.4 Configuring the IO cycle time

The CPU supplies a PROFINET IO device with new data within an IO cycle time period. The update time can be separately configured for each device and determines the time interval in which data is transmitted from the CPU to and from the device.

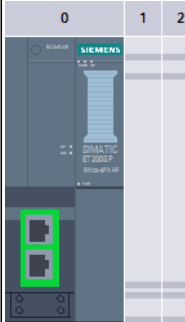
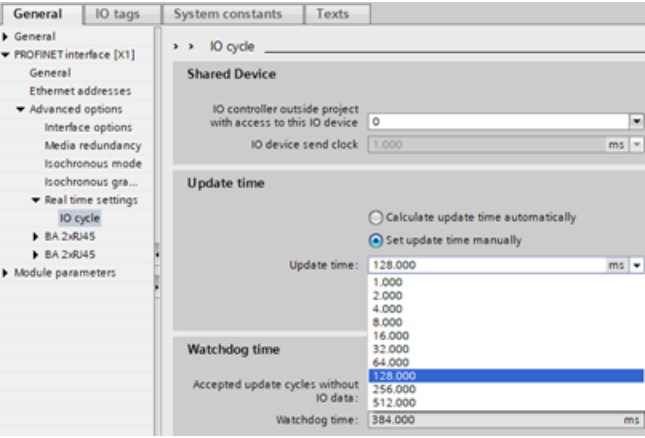
STEP 7 calculates the IO cycle update time automatically in the default setting for each device of the PROFINET network, taking into account the volume of data to be exchanged and the number of devices assigned to this controller. If you do not want to have the update time calculated automatically, you can change this setting.

To access the IO cycle parameters, click a PROFINET port on the ET 200SP IO device. From Properties dialog, select "Advanced options > Realtime settings > IO cycle".

Define the IO cycle "Update time" with the following selections:

- To have a suitable update time calculated automatically, select "Calculate update time automatically".
- To set the update time yourself, select "Set update time manually" and choose the required update time in ms from the dropdown menu.

Table 7-8 Configuring the ET 200SP PROFINET IO cycle time

ET 200SP PROFINET IO device	ET 200SP PROFINET IO cycle dialog
	

7.6.12.5 Prioritized startup of an IO device

IO devices can use "Prioritized Startup" (https://docs.tia.siemens.cloud/access?ft:originId=/10866368523/22911324171_enUS.htm&ft:clusterId/10866368523/22911324171.htm)" to reduce CPU connection time during power-up. With an S7-1200 G2 CPU, selecting this option implements Accelerated Startup instead of Fast Startup. Accelerated Startup provides faster device initialization than standard startup, but does not utilize DCP Hello messages to establish communication.

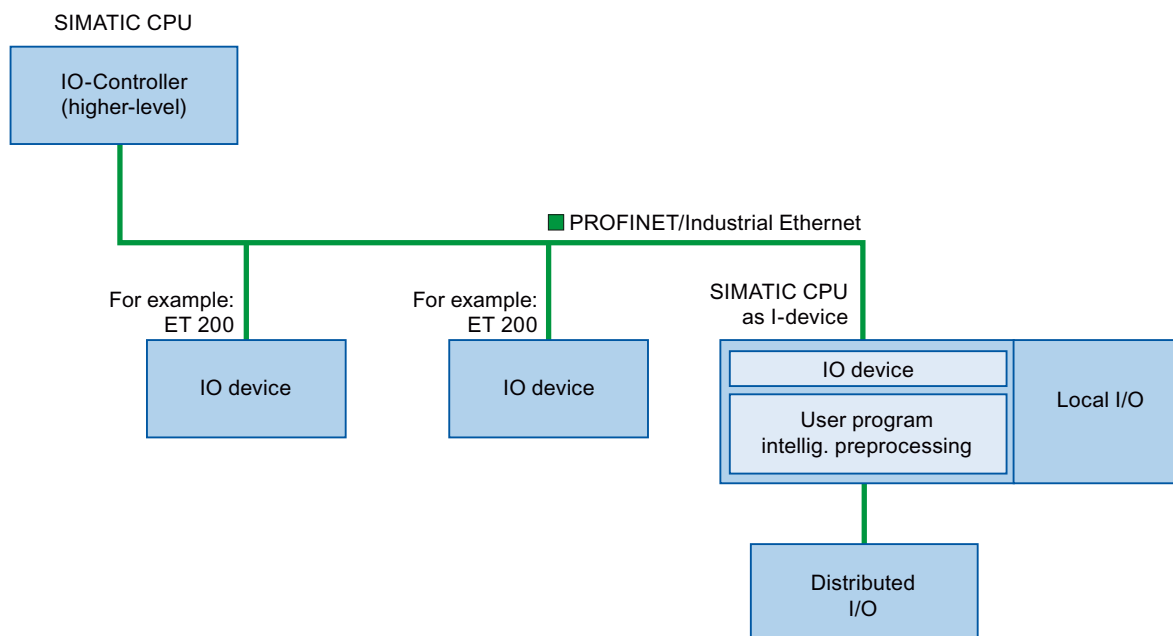
7.6.13 Configuring a CPU and PROFINET I-device

7.6.13.1 I-device functionality

A CPU with I-device functionality is called an "I-device".

The "I-device" (intelligent IO device) functionality of a CPU facilitates data exchange with an IO controller and operation of the CPU as an intelligent preprocessing unit of subprocesses, for example. The I-device is linked as an IO device to a "higher-level" IO controller.

STEP 7 handles the preprocessing on the CPU. The process values acquired in the local or distributed (PROFINET IO) I/O are preprocessed by STEP 7 and made available through a PROFINET IO interface to the CPU of a higher-level station.



The S7-1200 G2 CPU can act as an I-device with PROFI-Energy functionality.

7.6.13.2 Properties and advantages of the I-device

The I-device allows you to separate STEP 7 automation projects between creators and users, with the GSD file serving as the interface between these projects. This establishes a connection to standard IO controllers through a standardized interface. Additionally, the I-device has a deterministic PROFINET IO system for real-time communication through the PROFINET IO interface.

Advantages

The I-device offers the following advantages:

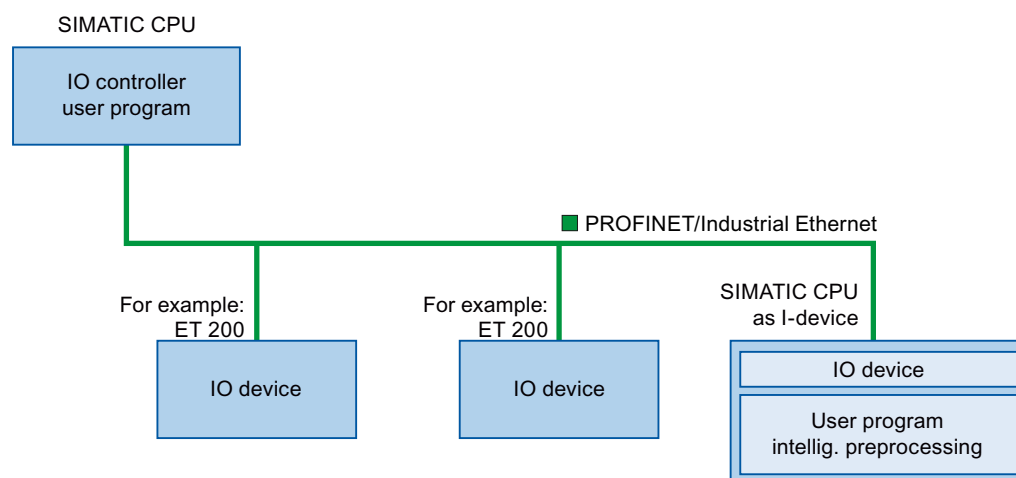
- Simple linking of IO controllers
- Real-time communication between IO controllers
- Relieving the IO controller by distributing the computing capacity to I-devices
- Lower communications load by processing process data locally
- Manageable solution design that includes the following:
 - Distributed processing: Divide complex automation tasks into smaller subprocesses for increased manageability and simplified subtasks.
 - Separating subprocesses: You can subdivide complicated, widely distributed and extensive processes into subprocesses with manageable interfaces by using I-devices. Store these subprocesses in separate STEP 7 projects and later merge them into a single master project.
 - Know-how protection: Deliver components with a GSD file for the I-device interface description instead of a STEP 7 project. This approach protects your program and eliminates the need for program publication.

7.6.13.3 Characteristics of an I-device

An I-device is included in an IO system like a standard IO device.

I-device without lower-level PROFINET IO system

The I-device does not have its own distributed I/O. The configuration and parameter assignment of the I-devices in the role of an IO device is the same as for a distributed I/O system (for example, ET 200).

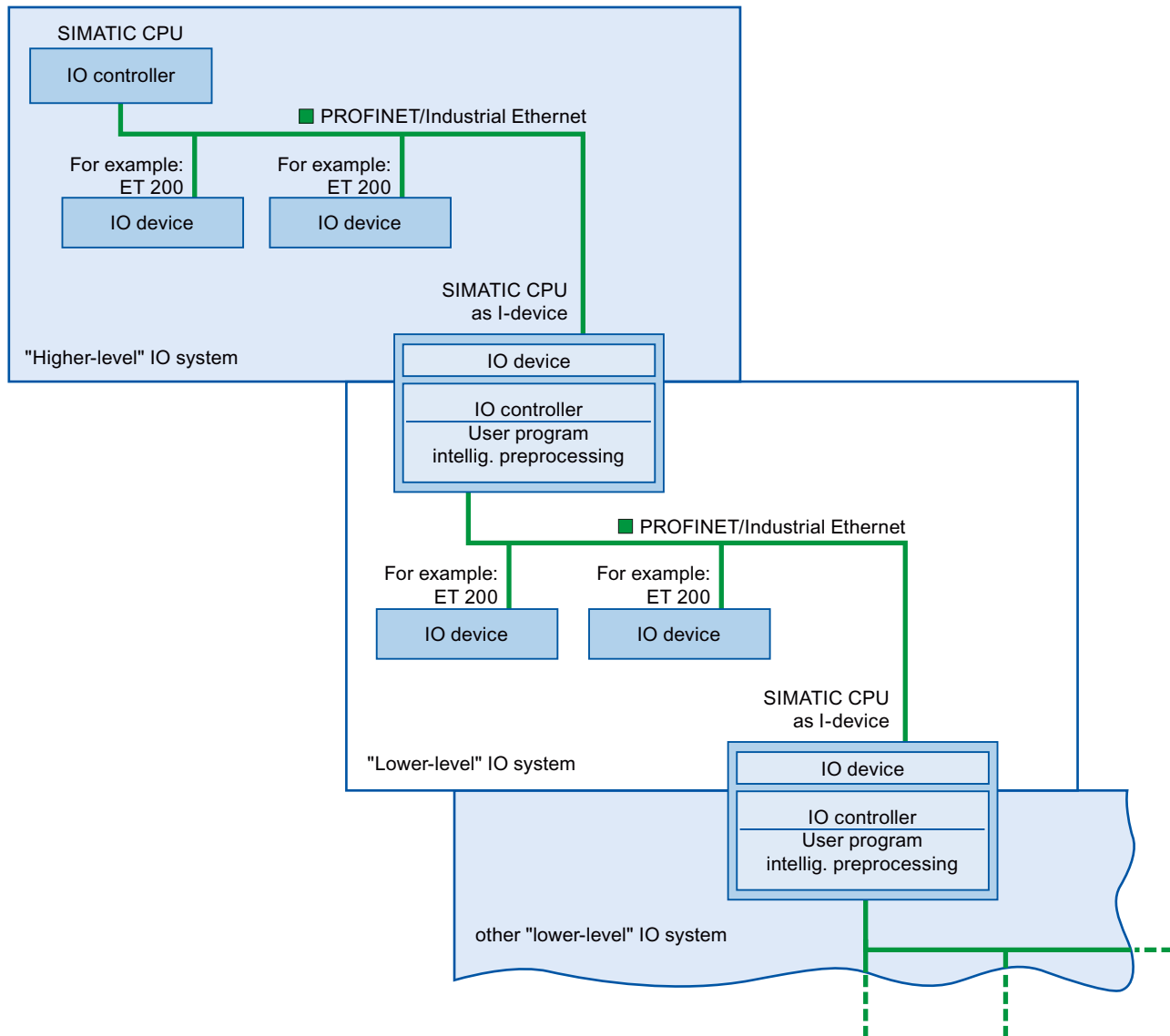


I-device with lower-level PROFINET IO system

Depending on the configuration, an I-device can also be an IO controller on a PROFINET interface in addition to having the role of an IO device.

This means that the I-device can be part of a higher-level IO system through its PROFINET interface and as an IO controller can support its own lower-level IO system.

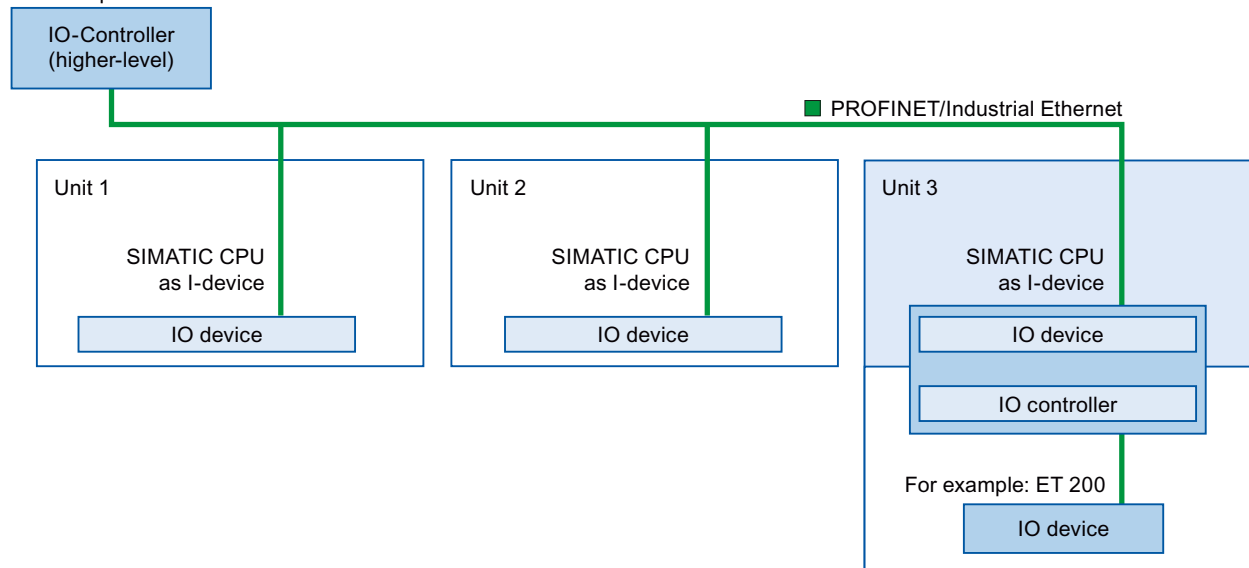
The lower-level IO system can, in turn, contain I-devices. This makes hierarchically structured IO systems possible.



Example: I-device as IO device and IO controller

This example explains the use of an I-device as IO device and IO controller in a print process. The I-device controls a unit (a subprocess). One unit is used, for example, to insert additional sheets such as flyers or brochures in a package of printed material.

For example: S7mEC



Unit 1 and unit 2 each consist of an I-device with local I/O. The I-device along with the distributed I/O system (for example, ET 200) forms unit 3.

The STEP 7 program on the I-device is responsible for preprocessing the process data. For this task, the STEP 7 program of the I-device requires default settings (for example, control data) from the higher-level IO controller. The I-device provides the higher-level IO controller with the results (for example, status of its subtask).

7.6.13.4 Data exchange between higher- and lower-level IO system

Transfer areas are an interface to the STEP 7 program of the I-device CPU. The CPU processes the inputs and sets the outputs.

The data for communication between IO controller and I-device is available in the transfer areas. A transfer area contains an information unit that is exchanged consistently between IO controller and I-device (Page 260).

Input transfer areas behave differently upon network loss between controller and I-device

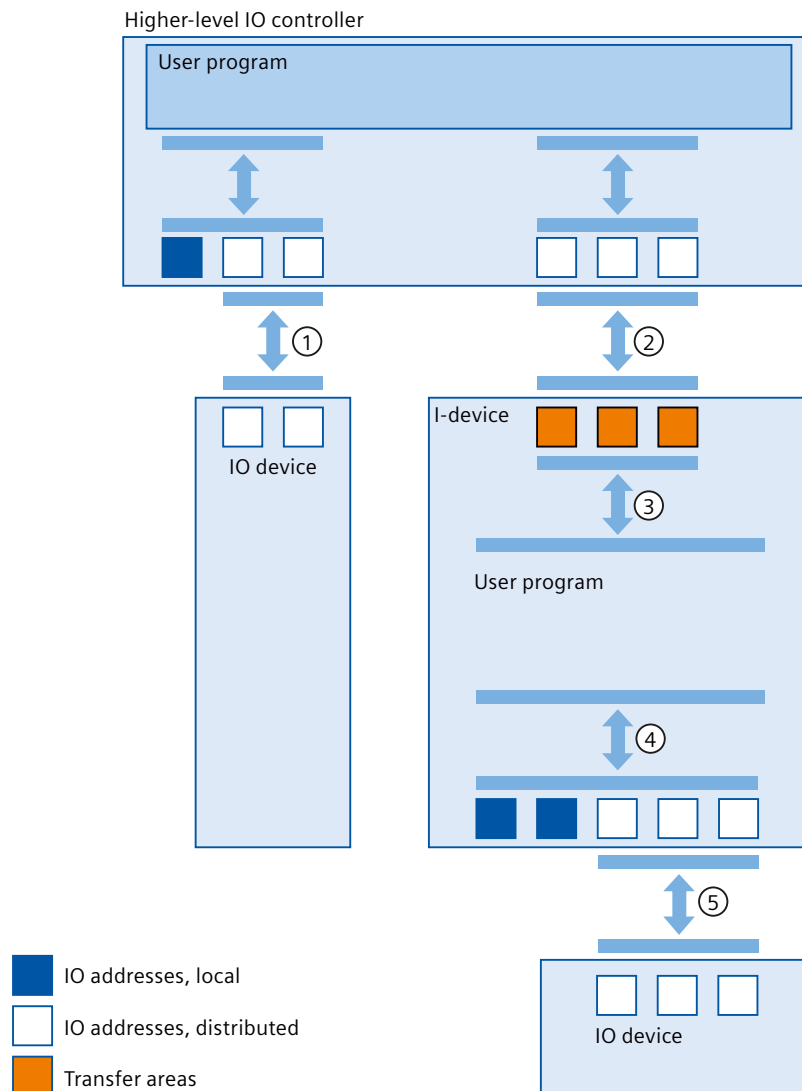
On the controller, the CPU writes zero to the input transfer areas upon network loss. On the I-device, the input transfer areas retain their last values.

You can configure your system to avoid this condition for the general I-device case (non-shared I-device). To do this, clear the input transfer areas for the I-device in a "Rack or Station Failure OB" for a coming event. Follow these steps:

1. Add a "Rack or Station Failure OB (Page 114)" to your project.
2. Add logic to the OB to write the values of the inputs for the I-device to zero when the startup variable of LADDR indicates the value of the I-device hardware ID and the startup variable of Event_Class indicates a "coming" event:
 - You can find the I-device hardware ID in the Default tag table in the "System constants" tab. The hardware ID is a type of "HW_Device", and the name of the tag indicates that it is an I-device (for example, "Local~PROFINET_interface_1~IODevice").
 - A value of "16#39" in the Event_Class indicates a "coming" event. If the "Event_Class" input variable contains the value of "16#39", this indicates that the "Rack or Station Failure OB" is now active (as opposed to being cleared).

Data exchange flow

The data exchange between the higher- and lower-level IO system is as follows:



- ① **Data exchange between higher-level IO controller and IO-device** through PROFINET.
- ② **Data exchange between higher-level IO controller and I-device** through PROFINET.
The data exchange between a higher-level IO controller and an I-device is based upon the conventional IO controller / IO device relationship.
For the higher-level IO controller, the transfer areas of the I-devices represent submodules of a preconfigured station.
The output data of the IO controller is the input data of the I-device. Similarly, the input data of the IO controller is the output data of the I-device.
- ③ **Transfer relationship between the STEP 7 program and the transfer area**
STEP 7 and the transfer area exchange input and output data.
- ④ **Data exchange between the STEP 7 program and the I/O of the I-device**
STEP 7 and the local / distributed I/O exchange input and output data.
- ⑤ **Data exchange between the I-device and a lower-level IO device** through PROFINET.

7.6.13.5 Configuring the I-device

You have two possibilities for configuration:

- Configuration of an I-device within a project
- Configuration of an I-device that is used in another project or in another engineering system

STEP 7 allows you to configure an I-device for another project or for another engineering system by exporting a configured I-device to a GSD file. You import the GSD file in other projects or engineering systems as with other GSD files. The transfer areas for the data exchange, among other data, are stored in this GSD file.

NOTE

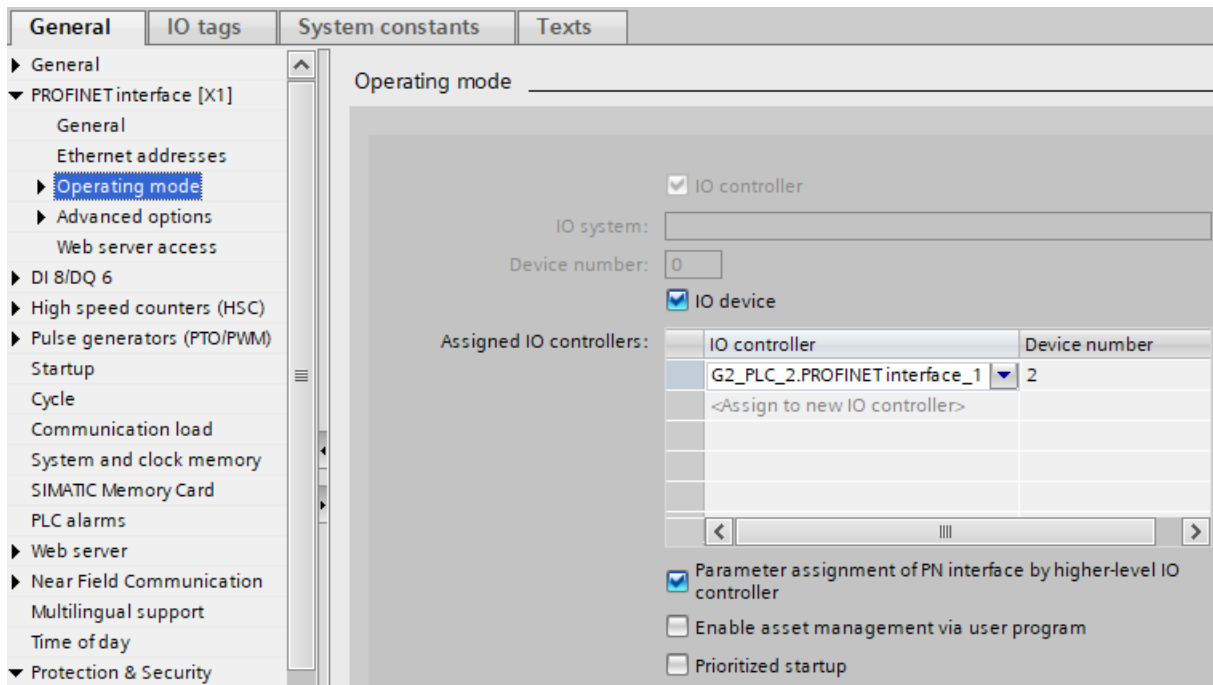
When you use the S7-1200 G2 as a shared I-device and as a controller, ensure that you increase the PROFINET I-device and PROFINET IO update times to alleviate the communications performance impact. The system is very stable and works well when you select 2 ms for the update time of a single PROFINET device time and you select 2 ms for the update time of a single PROFINET IO time.

Configuration of an I-device within a project

1. Drag-and-drop a PROFINET CPU from the hardware catalog into the network view.
2. Drag-and-drop the second PROFINET CPU, which can also be configured as an IO device, from the hardware catalog into the network view. This device is configured as an I-device (for example, CPU 1212C).
3. Click the device in the Device view to display the "Properties" tab view.
4. In the left column, select and expand the PROFINET interface for the I-device and select the "Operating Mode" category.
5. In the inspector window, select the checkbox for "IO device".

6. Choose the IO controller in the "Assigned IO controller" drop-down list.

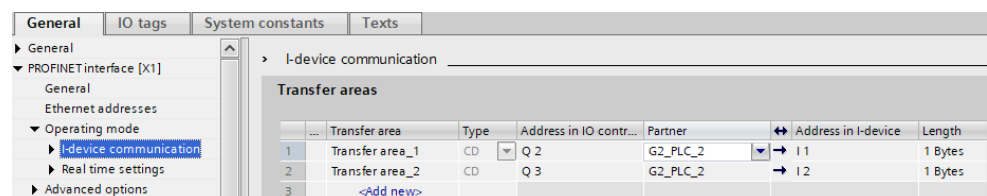
After you have chosen the IO controller, the network view displays the networking and the IO system between both devices.



7. With the "Parameter assignment of PN interface by higher-level IO controller" checkbox, you specify whether the interface parameters will be assigned by the Idevice or by a higher-level IO controller.

If you operate the I-device with a lower-level IO system, then the parameters of the I-device PROFINET interface (for example, the port parameter) cannot be assigned with the higher-level IO controller.

8. Configure the transfer areas. The transfer areas are found in the area navigation section "I-device communication":
 - Click in the first field of the "Transfer area" column. STEP 7 assigns a default name, which you can change.
 - Type of communication relation is set to CD (Communication Direction) by default.
 - Addresses are automatically preset; you can correct addresses if necessary, and determine the length of the transfer area which is to be consistently transferred.



9. A separate entry is created under "I-device communication" for each transfer area. If you select one of these entries, you can adjust the details of the transfer area, or correct them and comment on them.

NOTE

If you configure an S7-1200 G2 as an I-device, the maximum size of a transfer area is 1024 input or output bytes. There are possible constraining factors depending on local I/O as well as address space limitations on the controlling device.

Configuring an I-device with a GSD file

If you use an I-device in another project, or if the I-device is used in another engineering system, you must configure the higher-level IO controller and the I-device as follows:

1. Configure the transfer areas so the I-device creates a new GSD file (https://docs.tia.siemens.cloud/access?ft:originId=../10866368523/26415319307_enUS.htm&ft:clusterId../10866368523/26415319307.htm). This GSD file represents the configured I-device in other projects.
2. Assign a name for the I-device proxy as well as a description in the fields provided.
3. Click the "Export" button in the "I-device communication" section of the Inspector window.

To test, import the GSD file, for example, in another project.

7.6.14 Shared device functionality

Large or widely distributed systems might use multiple IO controllers.

By default, one IO controller manages each IO module of an IO device. The "Shared Device" function allows you to divide the modules or submodules of an IO device among different IO controllers.

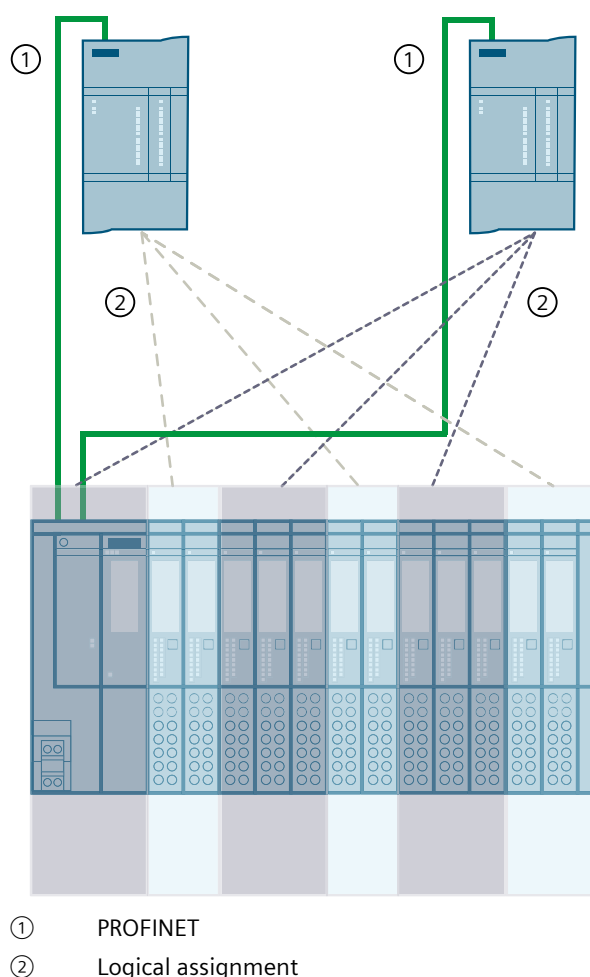
Configuration

When you configure an S7-1200 G2 CPU as an I-device, it enables the support of shared I-device functionality

(https://docs.tia.siemens.cloud/access?ft:originId=../10866368523/159334733835_enUS.htm&ft:clusterId=../10866368523/159334733835.htm) for up to two IO controllers. If both the IO controllers and the I-device are SIMATIC CPUs, configure them within a single STEP 7 project.

If one or both IO controllers are non-SIMATIC CPUs, use a GSD file for the configuration process

(https://docs.tia.siemens.cloud/access?ft:originId=../10866368523/59728529419_enUS.htm&ft:clusterId=../10866368523/59728529419.htm).



7.6.15 Media Redundancy Protocol (MRP)

The S7-1200 G2 CPUs support Media Redundancy Protocol (MRP) functionality and MRP ring setup as either a "Manager" or a "Client":

Media Redundancy Protocol	CPU as a Client	CPU as a Manager or Manager (Auto)
Functionality	Must operate in an MRP ring by forwarding MRP packets over its interface and reporting connection breaks to a manager in the network.	Must send MRP packets around the network, detect open ports in the ring, and manage blocked ports. Manager (Auto) only: Negotiate manager status with other potential managers.
Ring setup	Forwards test frames instead of making the check itself.	Uses test frames to check and make sure the ring is not interrupted.

Use the MRP protocol and configuration parameters (https://docs.tia.siemens.cloud/access?ft:originId=/10866368523/20055466635_enUS.htm&ft:clusterId/10866368523/20055466635.htm) to initialize MRP client and manager operation.

7.6.16 Media Redundancy with Planned Duplication of frames (MRPD)

The MRP extension "Media Redundancy with Planned Duplication of frames" (MRPD) (https://docs.tia.siemens.cloud/access?ft:originId=/10866368523/89155688459_enUS.htm&ft:clusterId/10866368523/89155688459.htm) provides the advantage that, in the case of a failure of a device or a line in the ring, all other devices continue to be supplied with IO data without interruption and with short update times.

MRPD is based on IRT and MRP. To realize media redundancy with short update times, the PROFINET devices participating in the ring send their data in both directions. The devices receive this data at both ring ports so that there is no reconfiguration time.

Requirements for media redundancy with MRPD

- All the devices of the ring must support MRPD. Terminal devices at the switch that cyclically exchange IRT data with a ring component must also support MRPD. MRPD support is listed in the device information in the STEP 7 hardware catalog (Devices & networks).
- You have configured MRP for all the devices of the ring.
- You have assigned the MRP role "Not device in the ring" to devices that are not located in the ring.
- You have configured IRT for all the involved components.

Configuring MRPD

You do not have to activate MRPD in STEP 7. The function is available automatically as soon as all the requirements for MRPD are fulfilled.

7.6.17 S7 routing

The S7-1200 G2 CPU supports S7 routing (https://docs.tia.siemens.cloud/access?ft:originId=../20713735819/26747797643_enUS.htm&ft:clusterId../20713735819/26747797643.htm) for up to 16 connections. When you have at least two PROFINET interfaces and up to three CP devices installed, the S7-1200 G2 CPUs offer two routing options within the station:

- Between the CPU and a CP
- From one CP to another CP

NOTE

You must add at least one CP.

7.6.18 Isochronous Real-Time PROFINET (IRT)

The S7-1200 G2 CPUs support Isochronous Real-Time PROFINET (IRT).

IRT is a transmission method by which PROFINET devices are synchronized with very high accuracy. A sync master specifies the clock to which sync slaves are synchronized. An IO controller or an IO device can have the role of sync master.

Sync master and sync slaves are always devices in a sync domain. Bandwidth is reserved within the sync domain for IRT communication. Real-time and non-real-time communication (TCP/IP communication) is possible outside of the reserved bandwidth.

PROFINET with IRT

(https://docs.tia.siemens.cloud/access?ft:originId=../10866368523/39589711499_enUS.htm&ft:clusterId../10866368523/39589711499.htm) is especially suited for the following:

- High performance and deterministics for large quantity structures with regard to user data communications (productive data).
- High performance even with many devices in the line topology with regard to user data communications (productive data).
- Parallel transmission of production and TCP/IP data over wire, and securing the forwarding of production data when data volume is high by reserving transmission bandwidth.

7.6.19 SNMP

Simple Network Management Protocol (SNMP) is an Internet standard protocol for collecting and organizing information about managed devices on IP networks and for modifying that information to change device behavior. Devices that typically support SNMP include routers, switches, servers, workstations, printers, modem racks, and more.

Network management systems use SNMP to monitor network-attached devices for conditions that warrant administrative attention. SNMP uses various services and tools for detection and diagnostics of the network topology. You can find information about the properties of devices capable of SNMP in the Management Information Base (MIB) files. You must have the required rights to access the MIB files.

SNMP exposes management data in the form of variables on the managed systems, which describe the system configuration. Managing applications can query (and sometimes set) these variables.

SNMP uses the UDP transport protocol and has two network components:

- **SNMP manager:** Monitors the network nodes
- **SNMP client:** Collects the various network-specific information in the individual network nodes and stores it in a structured form in the Management Information Base (MIB). You can use this data to perform detailed network diagnostics.

For security reasons, SNMP is disabled by default on S7-1200 G2 CPUs, preventing read and write access of SNMP variables. You must enable SNMP to remotely view and edit SNMP variables.

After enabling SNMP, certain conditions might require you to disable it. Examples of these conditions include the following:

- The security settings in your network do not allow the use of SNMP.
- You use your own SNMP solution (for example, with your own communications instructions).

If SNMP is disabled on the device, some functions and tools that rely on access to SNMP variables are unavailable or inoperable. For example, topology detection in TIA Portal is inoperable, and some functions of the SIMATIC Automation Tool V4.x and prior, are inoperable.

NOTE

Restoring the CPU to factory defaults disables SNMP.

Enabling and disabling SNMP from the device configuration

To enable or disable SNMP follow these steps:

1. From the Project Tree, under the CPU, double-click Device configuration.
2. From the General tab of the device properties, expand Advanced configuration and select SNMP.
3. To enable SNMP, select the "Activate SNMP" checkbox or to disable SNMP, deselect it.
4. Enter a Read-only community string or use the default (public) and enter a Read-write community string or use the default (private).

NOTE

To share SNMP data between the STEP 7 project and the PLC, the community name entered in the STEP 7 project must match the community name entered for the host when creating the SNMP database connection.

5. Download the configuration to the CPU.

Enabling and disabling SNMP from the STEP 7 program

For detailed information on enabling and disabling SNMP from your STEP 7 program, see the following areas in the TIA Portal Information System:

- Configuring SNMP
(https://docs.tia.siemens.cloud/access?ft:originId=../52499730827/59148451211_enUS.htm&ft:clusterId../52499730827/59148451211.htm)
- Activating and deactivating SNMP
(https://docs.tia.siemens.cloud/access?ft:originId=../11627607179/90872859787_enUS.htm&ft:clusterId../11627607179/90872859787.htm)
- Disabling SNMP: Full program example
(https://docs.tia.siemens.cloud/access?ft:originId=../11627607179/96590122635_enUS.htm&ft:clusterId../11627607179/96590122635.htm)

7.7 S7 communication

7.7.1 PUT and GET (Write and read from a remote CPU)

You can use the PUT and GET instructions to communicate with S7 CPUs through PROFINET connections. This is only possible if the "Permit access with PUT/GET communication from remote partner" function is activated for the partner CPU in the "Protection & Security" property of the local CPU properties:

- Accessing data in a remote CPU: An S7-1200 G2 CPU can only use absolute addresses in the ADDR_x input field to address variables of remote CPUs (S7-200/300/400/1200).
- Accessing data in a standard DB: An S7-1200 G2 CPU can only use absolute addresses in the ADDR_x input field to address DB variables in a standard DB of a remote S7 CPU.
- Accessing data in an optimized DB: An S7-1200 G2 CPU cannot access DB variables in an optimized DB of a remote S7-1200 G2 CPU.
- Accessing data in a local CPU: An S7-1200 G2 CPU can use either absolute or symbolic addresses as inputs to the RD_x or SD_x input fields of the PUT or GET instruction, respectively.

Enabling PUT/GET access

PUT/GET operation is not automatically enabled.

To enable PUT/GET access, follow these steps:

1. In the Project tree under "Security settings" > "Users and roles", click the checkbox to enable the Anonymous user.
2. In the "Roles" tab, click "Add new role" and give it a name.
3. From the "Roles" tab, click the "Runtime rights" tab and select your PLC from the dropdown menu at left.
4. Assign at least one of the following function rights for your PLC:
 - HMI access
 - Read Access
 - Full access

5. Select the "Users" tab in the top right and click the checkbox beside the new role to assign it to the Anonymous user.
6. In the CPU's "Device configuration" inspector window, select the "Properties" tab > "Protection & Security > Connection mechanisms" and click the checkbox to "Permit access with PUT/GET communication from remote partner".

WARNING

Avoiding security risks from network attacks

If an attacker can access your networks, the attacker can possibly read and write data.

For example, I/O exchange through PROFINET, PUT/GET, T-Block, and communication modules (CMs) have no security features. You must protect these forms of communication.

If you fail to protect these forms of communication, death or severe personal injury can result.

For security information and recommendations, see the "Operational Guidelines

(<https://www.siemens.com/global/en/products/services/cert/news/operational-guidelines-for-industrial-security.html>)" white paper on the Siemens Industrial Cybersecurity Web site.

Protocol

The protocol for S7 communication and communication instructions are as follows:

Protocol	Usage examples	Entering data in the receive area	Communication instructions	Addressing type
S7 communication	CPU-to-CPU communication Read/write data from/to a CPU	Data transmission and reception with specified length	PUT and GET	Assigns TSAPs to the Local (active) and Partner (passive) devices

Instructions

The S7 communication

(https://docs.tia.siemens.cloud/access?ft:originId=/15891429899/15891429899_enUS.htm&ft:clusterId/15891429899/15891429899.htm) PUT and GET instructions allow you to read and write data from a remote CPU:

Communication	
Name	Description
S7 communication GET PUT	Read data from a remote CPU Write data to a remote CPU
Open user communication	
OPC UA	
WEB Server	
Others	
Communication processor	
TeleService	

7.7.2 Creating an S7 connection

You must have permission to access remote connection partners with PUT/GET instructions.

By default, the "Permit access with PUT/GET communication from remote partner" option is disabled. In this case, read and write access to CPU data is only possible for communication connections that require configuration

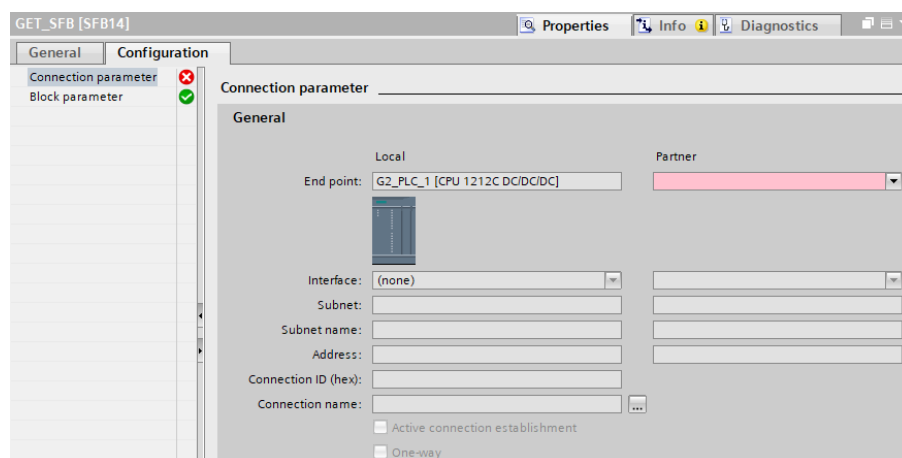
(https://docs.tia.siemens.cloud/access?ft:originId=../10866368523/25480655883_enUS.htm&ft:clusterId/10866368523/25480655883.htm) or programming both for the local CPU and for the communication partner.

7.7.3 PUT/GET connection parameter assignment

The PUT/GET instructions connection parameter assignment is a user aid for configuring CPU-to-CPU S7 communication connections.

After inserting a PUT or GET instruction, the Properties tab for the instruction displays the connection parameter assignment dialog for the GET/PUT instructions.

The "Connection parameters" dialog allows you to configure the necessary S7 connection and to configure the parameter "Connection ID" that is referenced by the GET/PUT block parameter "ID". The dialog has information about the local endpoint and allows you to define the local interface. You can also define the partner end point.



The "Block parameters" dialog allows you to configure the additional block parameters.

Table 7-9 Connection parameter: General definitions

Parameter		Definition
Connection parameter: General	End point	"Local End point": Name assigned to the Local CPU "Partner End point": Name assigned to the Partner (remote) CPU Note: In the "Partner End point" dropdown list, the system displays all potential S7 connection partners of the current project as well as the option "unspecified". An unspecified partner represents a communication partner which is not currently in the STEP 7 project (for example, a third party device communication partner).
	Interface	Name assigned to the interfaces Note: You can change the connection by changing the Local and Partner interfaces
	Subnet	Type of subnet
	Subnet name	Name assigned to the subnets

Parameter		Definition
Connection parameter: General	Address	Assigned IP addresses Note: You can specify the remote address of a third party device for an "unspecified" communication partner.
	Connection ID (hex)	ID number: Automatically generated by the GET/PUT connection parameter assignment
	Connection name	Local and Partner CPU data storage location: Automatically generated by the GET/PUT connection parameter assignment
	Active connection establishment	Checkbox to select Local CPU as the active connection
	One-way	Checkbox to specify a one-way or two-way connection; read-only Note: In a PROFINET GET/PUT connection, both the local and partner devices can act as a server or a client. This allows a two-way connection, and the "One-way" checkbox is unchecked.

7.7.3.1 Connection ID parameter

You can change the system-defined connection IDs in one of the following ways:

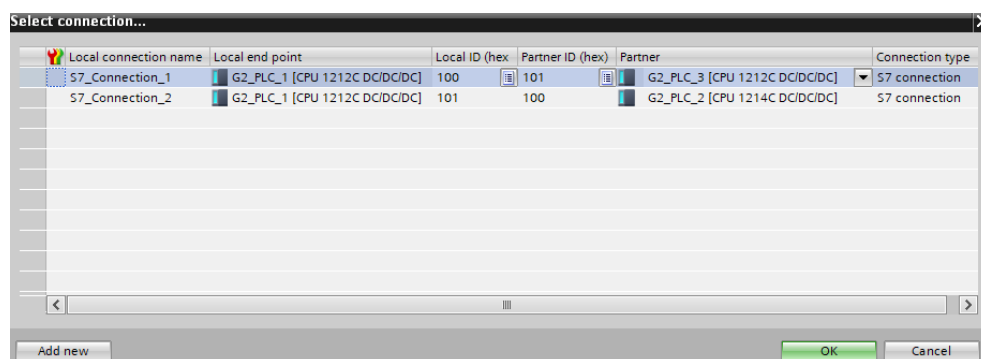
- Change the current ID directly on the GET/PUT instruction. If the new ID belongs to an already existing connection, the connection is changed.
- Change the current ID directly on the GET/PUT instruction, but the new ID does not already exist. A new S7 connection is created by the system.
- Change the current ID through the "Connection overview" dialog: Your input is synchronized with the ID-parameter on the corresponding GET/PUT instruction.

NOTE

The parameter "ID" of the GET/PUT instruction is not a connection name, but a numerical expression, which is written like the following example: W#16#1

7.7.3.2 Connection name parameter

The connection name is editable through the "Select connection" dialog. This dialog offers all the available S7 connections that could be selected as an alternative for the current GET/PUT communication. You can create a new connection in this table. Click the button to the right of the "Connection name" field to start the "Select connection" dialog.



7.8 Diagnostic events for distributed I/O

As shown in the following table, the CPU supports diagnostics that can be configured for the components of the distributed I/O system. Each of these errors generates a log entry in the diagnostics buffer.

Table 7-10 Handling of diagnostic events for PROFINET

Type of error	Diagnostic information for the station?	Entry in the diagnostics buffer?	CPU operating mode
Diagnostic error	Yes	Yes	Stays in RUN mode
Rack or station failure	Yes	Yes	Stays in RUN mode
I/O access error ¹	No	Yes	Stays in RUN mode
Peripheral access error ²	No	Yes	Stays in RUN mode
Pull / plug event	Yes	Yes	Stays in RUN mode

¹ I/O access error example cause: Reading inputs or writing outputs for a module that has been removed or not communicating.

² Peripheral access error example cause: Reading peripheral inputs or writing peripheral outputs for a module that has been removed or not communicating.

Use the GET_DIAG instruction for each station to obtain the diagnostic information. This will allow you to programmatically handle the errors encountered on the device and if desired take the CPU to STOP mode. This method requires you to specify the hardware device from which to read the status information.

The GET_DIAG instruction uses the "L address" (LADDR) of the station to obtain the health of the entire station. This L Address can be found within the Network Configuration view and by selecting the entire station rack, the L Address is shown in the Properties Tab of the station. The LADDR for each individual module is either in the properties for the module in the device configuration or in the default tag table for the CPU.

7.9 What to do when you cannot access the CPU by the IP address

In case you cannot reach a CPU by the IP address, you can set an emergency (temporary) IP address for the CPU. The emergency IP address enables you to re-establish communication with the CPU in order to download a device configuration with a valid IP address.

Reasons why you might need an emergency IP address

Your CPU might be inaccessible if someone downloaded a project with one of the following problems:

- The IP address of the PROFINET interface of the CPU is a duplicate of another device on the network.
- The subnet is incorrect for the CPU.
- The subnet mask makes the CPU unreachable.

In these cases, the CPU is no longer accessible from STEP 7.

Assigning an emergency IP address

You can assign an emergency IP address under the following conditions:

- The device configuration in STEP 7 has "Set IP address in the project" for the IP protocol.
- The CPU is in STOP mode.

Under these conditions, you can use a DCP tool to set the IP address of the device to an emergency IP address. The SIMATIC Automation Tool, for example, has a DCP Set IP address command. You can set an emergency IP address regardless of the protection level of the CPU. After you set a temporary IP address with a DCP tool, the Maintenance LED on the CPU turns on. The Diagnostics Buffer also includes an entry indicating that you enabled an emergency address of an Ethernet interface.

Restoring an IP address after assigning an emergency IP address

The diagnostics buffer informs you when you have enabled or disabled an emergency IP address. You can reset the emergency IP address by powering the CPU off and on.

After you have assigned an emergency IP address, you can then download a STEP 7 project with a valid IP address for the CPU. After you download the project, power cycle the CPU.

7.10 OPC UA server

S7-1200 G2 CPUs support configuration as an OPC UA server (https://docs.tia.siemens.cloud/access?ft:originId=../19342675723/111512317451_enUS.htm&ft:clusterId/19342675723/111512317451.htm) for data access. For additional information on OPC UA servers, visit the OPC Foundation Web site (<https://opcfoundation.org/>).

S7-1200 G2 OPC UA server features

The S7-1200 G2 CPUs provide OPC UA server capabilities, including the following:

- Data access
- Diagnostics
- Server method support

OPC UA server configuration

The OPC UA server is deactivated by default. To use the OPC UA server, you must configure the OPC UA settings in STEP 7.

7.10.1 OPC UA Server method instructions

The OPC UA Server method instructions provide the capability to inject custom logic and checks before an OPC UA method (https://docs.tia.siemens.cloud/access?ft:originId=../19342675723/111512403723_enUS.htm&ft:clusterId/19342675723/111512403723.htm) is executed and to process its outcome or perform follow-up actions after it completes. These can be found in the following folders:{"OPC UA Server method instructions"}{"Instructions";"OPC UA Server method"}

Communication	
Name	Description
▶ S7 communication	
▶ Open user communication	
▼ OPC UA	
▼ OPC UA server	
■ OPC-UA_ServerMethodPre	Preparation of the server method call
■ OPC-UA_ServerMethodPost	Postprocessing of the server method call
▶ Others	
▶ Communication processor	

7.10.2 Limitations of the OPC UA server

When using OPC UA server interfaces, you must comply with the following limitations:

- Number of server interfaces
- Number of companion specifications
- Reference namespaces
- Number of OPC UA nodes
- Number of namespaces

NOTE

The S7-1200 G2 OPC UA server does not support the S7-1500 feature of "standard SIMATIC" server interface. You must define and download an OPC UA server interface in STEP 7.

Interface, method, and subscription limitations

The following tables apply to S7-1200 G2 CPUs and S7-1200 G2 Fail-safe CPUs. Consider these limitations when compiling and loading a configuration. Exceeding these limitations results in an error message.

Interface limitations	Description	Maximum
Number of server interfaces	The number of concurrent OPC UA server connections that can be established. A server interface can be a "Companion specification" type or a "Server interface" type.	2
Number of companion specifications	The number of extra templates or add-ons that your OPC UA server can use to share data.	2
Reference namespaces	Unique identifiers that organize related data items into separate groups.	10
Number of OPC UA nodes	The maximum number includes nodes internally defined by the server interface.	2000
Total number of namespaces	The total number of defined namespaces for all server interface types: "server interface", "companion specification", and "reference namespace"	18

Method limitations	Maximum
Server methods	20 ¹
Server method instance DBs for all server interfaces and associated server methods	20
Server method input arguments	20
Server method output arguments	20

¹ If you download a program with more than the maximum allowed OPC UA methods, the program cannot call any of the OPC UA methods.

Subscription limitations	Maximum
Concurrent subscriptions ¹	50
Subscriptions per session	5

¹ Concurrent subscriptions is equal to the configured number of concurrent sessions multiplied by the maximum number of subscriptions per session.

7.10.3 OPC UA server security

The OPC UA server requires a certificate for activation. When you activate the server, TIA Portal generates a certificate. You can change this certificate in the PLC properties.

Supported security policies

Selecting a supported security policy at runtime determines the security of communications (https://docs.tia.siemens.cloud/access?ft:originId=../19342675723/111512278283_enUS.htm&ft:clusterId../19342675723/111512278283.htm) between the client and server. The S7-1200 G2 supports the following security policies:

Security Policy	Enabled by default?
No security	No
Basic128Rsa15 - Sign	No
Basic128Rsa15 - Sign & Encrypt	No
Basic256 - Sign	No
Basic256 - Sign & Encrypt	No
Basic256Sha256 – Sign	No
Basic256Sha256 – Sign & Encrypt	Yes
Aes128-Sha256-RsaOaep - Sign	No
Aes128Sha256RsaOaep - Sign & Encrypt	No
Aes256Sha256RsaPss - Sign	No
Aes256Sha256RsaPss - Sign & Encrypt	No

Trusted Clients

You can accept client certificates using one of the following two methods from the "Trusted clients" window in your STEP 7 project:

- You can define a list of trusted clients by adding their certificates to the list. At runtime, only clients with a trusted certificate can connect.
- You can select the checkbox at the bottom of the window to "Automatically accept client certificates during runtime". At runtime, all client certificates are accepted automatically.

7.11 Communication Processor (CP)

7.11.1 CP 1243-1

The S7-1200 G2 Ethernet Communications Processor (CP) equips the S7-1200 G2 with an extra Ethernet interface. Through this interface, the CP establishes a reliable, secure link for data exchange and remote command execution, facilitating Industrial Remote Control (TeleControl) of S7-1200 G2 processes. The CP further supports web server access.

Ethernet CP for the S7-1200 G2

For TeleControl applications, the CP 1243-1 is available with details as follows:

- Article number: 6GK7243-1BX50-0XE0
- Communications processor for connecting the SIMATIC S7-1200 G2 to Industrial Ethernet or via the Internet to the DNP3 master station.
- You can use the CP as an interface extension of the CPU. In this role, it serves the purpose of network separation.
- You communicate between the CP and CPU using configurable data points that access PLC tags.

Secure communication

The well-proven SINAUT ST7 protocol or the standardized DNP3 or IEC 60870-5 protocol adds security to Industrial Remote Communication. The TeleControl solution provides comprehensive measures to prevent data falsification and loss. Each transmission module has a large memory for several thousand data frames, which offers the ability to bridge downtimes in the transmission link.

The TeleControl solution via DNP3 provides comprehensive measures to prevent data falsification and loss. Each transmission module has a large memory for several thousand data frames, which offers the ability to bridge downtimes in the transmission link. The DNP3 implementation also provides security via TLS.

Updating CP 1243-1 firmware

If you update the CP firmware, you must power cycle your PLC to activate the new firmware.

7.11.2 Further information

The SIMATIC CP 1243-1 (<https://sieportal.siemens.com/su/blZek>) manual provides detailed information on connection, requirements, applications, block instructions, accessories, and configuration examples.

For further information and documentation, visit the following:

- CP 1243-1 (<https://sieportal.siemens.com/su/blYx6>)
- Firmware updates as available (<https://sieportal.siemens.com/su/blYzU>)

7.12 Point-to-point (PtP) communication

7.12.1 Overview

The following table outlines the point-to-point (PtP) character-based serial protocols supported by the CPU, along with the available instruction sets and communication hardware options for each protocol.

Protocol	Instruction Folder	Local CM 1241 RS232/422/485	Local CB 1241 RS485	Distributed CM PtP (example: ET 200MP CM or ET 200SP CM)
Freeport (Page 281)	Communication > Communication processor > PtP communication	Yes	Yes	Yes
3964(R) (Page 295)	Communication > Communication processor > PtP communicaton	Yes (RS232 or RS422)	No	Yes (RS232 or RS422)
USS (Page 303)	Communication > Communication processor > USS communication	Yes (RS485)	Yes	Yes (RS485)

7.12.2 Using the serial communication interfaces

The CM 1241 RS232/422/485 ([Page 491](#)) and the CB 1241 RS485 ([Page 493](#)) provide the interface for Point-to-point (PtP) communications.

You can connect up to three CMs and the following number of CBs as serial communication interfaces:

- One CB for the 1212C or 1212FC CPUs
- Up to two CBs for the 1214C or 1214FC CPUs

Install the CM to the right of the CPU or another CM or CP. Install the CB(s) on the front of the CPU. Refer to the installation guidelines ([Page 74](#)) for information on module installation and removal.

The serial communication interfaces feature the following:

- Isolated port
- Support for Point-to-Point protocols
- Configuration and programming through the PtP communication processor instructions
- Display of transmit and receive activity, as well as diagnostics, by means of LEDs
- No external power connection is needed as they are powered by the CPU

Refer to the technical specifications for communication interfaces ([Page 489](#)).

LED indicators

The CM and CB each have three LED indicators:

- **Diagnostic LED (DIAG):** This LED flashes red until it is addressed by the CPU. After the CPU powers up, it checks for CM/CB and addresses them. The diagnostic LED begins to flash green. This means that the CPU has addressed the CM/CB, but has not yet provided the configuration to it. The CPU downloads the configuration to the configured CM/CB when the program is downloaded to the CPU. After a download to the CPU, if no errors are detected, the diagnostic LED on the communication module shows a steady green. If an error is detected, the diagnostic LED flashes red.
- **Transmit LED (Tx):** The transmit LED illuminates when data is being transmitted out the communication port.
- **Receive LED (Rx):** This LED illuminates when data is being received by the communication port.

7.12.3 Biasing and terminating an RS422 or RS485 network connector

Biasing

The S7-1200 G2 CM/CB includes built-in biasing functionality. This allows the CM/CB to automatically select and apply the appropriate biasing based on the mode or configuration you have selected and downloaded to the CPU from your STEP 7 project.

Terminating a network connector

To ensure optimal signal transmission and prevent signal reflections or interference, you must properly connect and terminate the ends of an RS422 or RS485 network connector.

To ensure interference-free data traffic for RS422 or RS485, add a terminating resistor of approximately 330Ω at the receiving end of the cable.

NOTE

When the parallel terminating resistor is wired in the circuit, you must enable the bias resistors in your STEP 7 project. Otherwise, data reads are incorrect because the receive buffer incorrectly detects the wrong start bit and bit-shifts the data being received.

You can use the following cable types with both RS422 and RS485 network connectors. The cable supports various lengths based on the baud rate as follows:

- Max. 1200 m at 19200 baud
- Max. 500 m at 38400 baud
- Max. 350 m at 76800 baud
- Max. 250 m at 115200 baud
- Max. 200 m at 250000 baud (RS485 only)

NOTICE

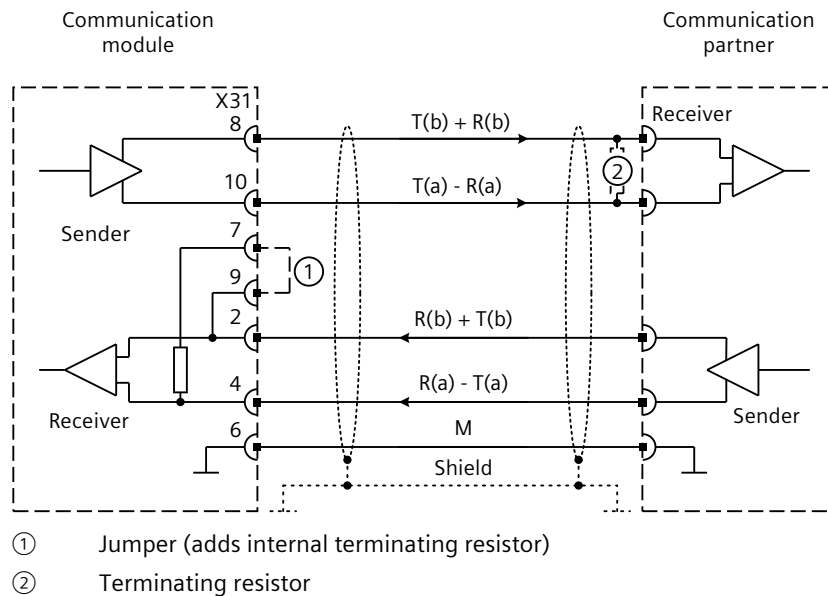
Risks of connecting a cable shield directly to the ground (GND)

Connecting a cable shield directly to the GND can cause electrical current induction, which could damage the expansion modules.

To mitigate this risks, connect the GND wire on both ends of the cable. This helps maintain a consistent ground potential and minimizes the chances of electrical current induction or other related issues that can affect the performance and reliability of the network connection.

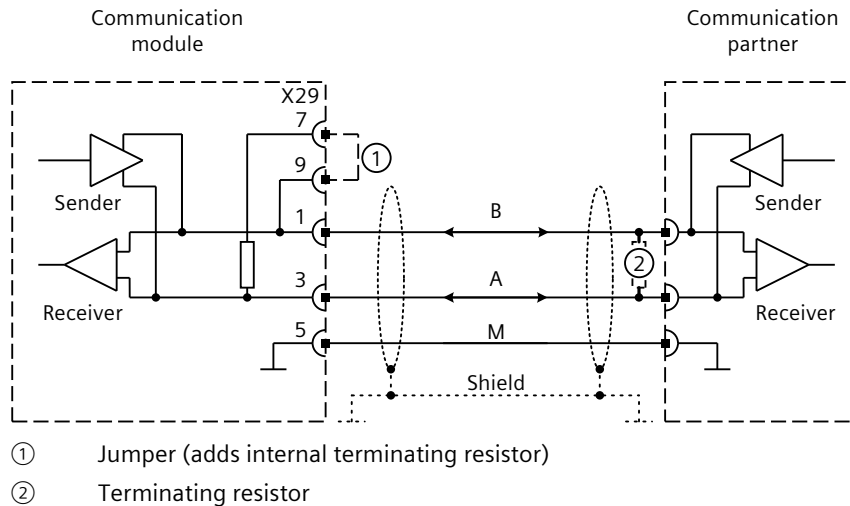
Terminating the RS422 network connector

You can configure the RS422 point-to-point connection cable as shown in the following example:



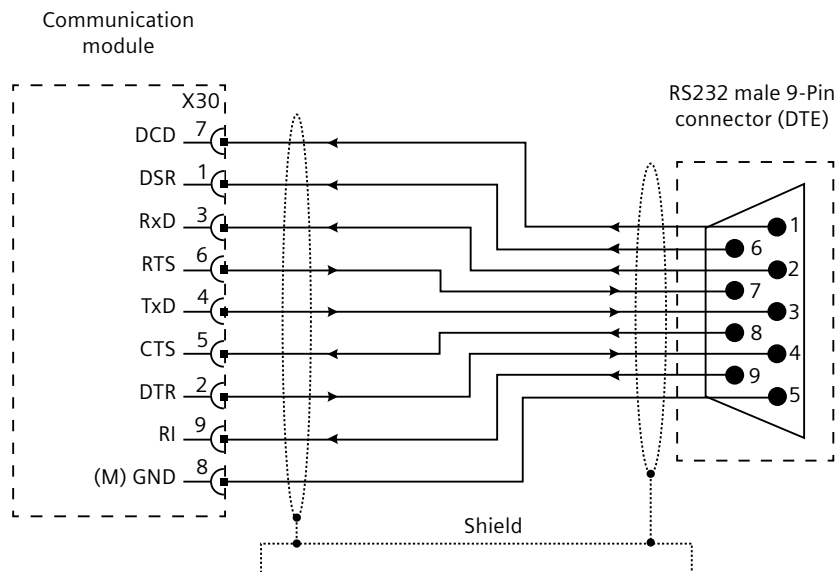
Terminating the RS485 network connector

You can configure the RS485 point-to-point connection cable as shown in the following example:



Connecting an S7-1200 G2 CPU to a 9-pin D connector

You can connect the S7-1200 G2 CPU to a standard RS232 DTE 9-pin D connector as shown in the following example:



Your application might not require all of these signal connections.

NOTE

The maximum cable length for this connection should not exceed 10 meters.

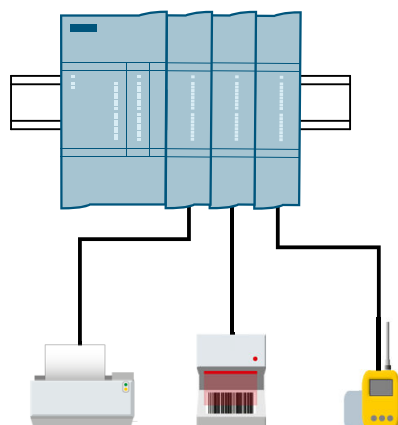
7.12.4 PtP, Freeport communication

PtP with a Freeport, or freely constructed, protocol provides maximum freedom and flexibility, but requires extensive implementation in the STEP 7 program.

PtP enables a wide variety of possibilities:

- The ability to send information directly to an external device such as a printer
- The ability to receive information from other devices such as barcode readers, RFID readers, third-party camera or vision systems, and many other types of devices
- The ability to exchange information, sending and receiving data, with other devices such as GPS devices, third-party camera or vision systems, radio modems, and many more

This type of PtP communication is serial communication that uses standard UARTs to support a variety of baud rates and parity options. The RS232/422/485 communication module (CM 1241) and the RS485 communication board (CB 1241) provide the electrical interfaces for performing the PtP communications.



PtP Freeport over PROFINET

PtP enables you to use a PROFINET distributed I/O rack to communicate to various devices (RFID readers, GPS device, and others). You connect the Ethernet interface of the S7-1200 G2 CPU to a PROFINET interface module. PtP communication modules in the rack with the interface module can then provide serial communications to the PtP devices.

Communications over distributed I/O use the following modules:

Station	Module	Article number	Interface
ET 200MP	CM PtP RS232 BA	6ES7540-1AD00-0AA0	RS232
	CM PtP RS232 HF	6ES7541-1AD00-0AB0	RS232
	CM PtP RS422/485 BA	6ES7540-1AB00-0AA0	RS422/RS485
	CM PtP RS422/485 HF	6ES7541-1AB00-0AB0	RS422/RS485
ET 200SP	CM PtP	6ES7137-6AA01-0BA0	RS232 and RS422/RS485

NOTE

You can use the same point-to-point instructions to access a communication board, local serial modules, and serial modules over PROFINET.

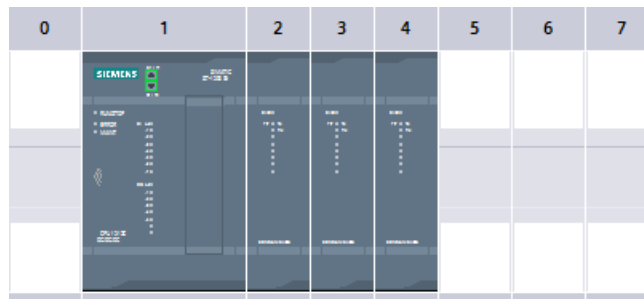
7.12.5 Configuring the PtP Freeport communication

7.12.5.1 Configuring the communication ports

You can use either of the following methods to configure the communication interfaces for PtP Freeport communication:

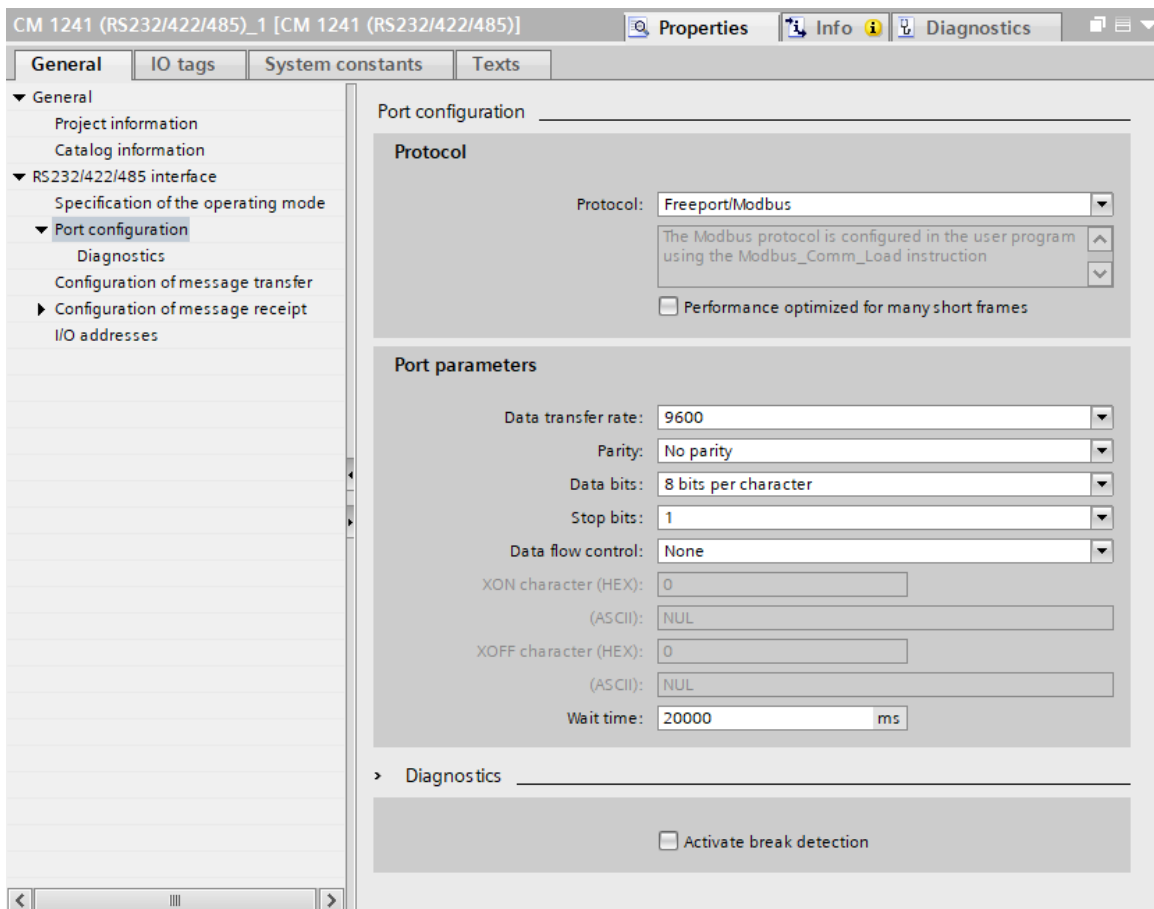
- Use the device configuration in STEP 7 to configure the port parameters (baud and parity), the send parameters, and the receive parameters. The CPU stores the device configuration settings and applies the settings after a power cycle and a RUN to STOP transition.
- Use the Port_Config, Send_Config, and Receive_Config instructions ([Page 300](#)) to set the parameters. The port settings set by the instructions are valid while the CPU is in RUN mode. The port settings revert to the device configuration settings after a STOP transition or power cycle.

After configuring the hardware devices ([Page 158](#)), select one of the configured CMs or CBs to configure parameters for the communication interfaces.



The "Properties" tab of the inspector window displays the parameters of the selected CM. Select "Port configuration" to edit the following parameters:

- Protocol - "Performance optimized for many short frames"¹
- Operating mode
- Data transmission rate
- Parity
- Data bits
- Stop bits
- Flow control - RS232 or RS422 only
- Wait time



The CB 1241 supports standard performance only; The CM 1241 supports both standard performance and "Performance optimized for many short frames". Optimized performance is faster but requires more process image space.

- Standard performance
 - Handshaking is done via the process image.
 - Data are sent via records.
- Optimized performance
 - Handshaking is done via the process image.
 - Data are sent via the process image.

For more information regarding the sending and receiving of data for both standard and optimized performance, see the the following chapters in the SIMATIC S7-1500, ET 200MP, ET 200SP CM PtP - Configurations for point-to-point connections Function manual (<https://support.industry.siemens.com/cs/us/en/view/59057093>):

- "Configuring/parameter assignment"
- "Programming - communication using instructions"

The STEP 7 program can also configure the port or change the existing configuration (https://docs.tia.siemens.cloud/access?ft:originId=, /39512235019/CM1500_Prog_Port_Config_enUS.htm&ft:clusterId=, /39512235019/CM1500_Prog_Port_Config.htm) with the Port_Config instruction.

Parameter	Definition
Protocol	This selects the Protocol Freeport/Modbus or 3964(R) (CM only).
Performance optimized for many short frames	Click the checkbox to optimize performance (CM only).
Operating mode	This selects the type of communication (RS232, RS422, or RS485) and the network configuration. The default mode for Operating mode is RS232 mode. Other valid choices are: • Full duplex (RS422) 4-wire operation point to point • Full duplex (RS422) 4-wire operation multipoint master • Full duplex (RS422) 4-wire operation multipoint slave • Half duplex (RS485) 2-wire operation
Data transfer rate	The default value for the data transmission rate is 9600 bits/s. Valid choices in bits/s are: • 300 • 600 • 1200 • 2400 • 4800 • 9600 • 19200 • 38400 • 57600 • 76800 • 115200 • 250000 (RS422 and RS485 only)

Parameter	Definition
Parity	The default value for parity is no parity. Valid choices are: - No parity - Even - Odd - Mark (parity bit always set to 1) - Space (parity bit always set to 0)
Data bits per character	The number of data bits in a character. Valid choices are 7 or 8.
Number of stop bits	The number of stop bits can be either 1 or 2. The default is 1.
Data flow control	The RS485 communication interfaces do not support flow control. The RS232 mode of the CM 1241 RS232/422/485 module allows you to select either hardware or software flow control (Page 285). If you select hardware flow control, you can select whether the RTS signal is always on, or RTS is switched. If you select software flow control, you can define the XON and XOFF characters. The RS422 mode of the CM 1241 RS232/422/485 module supports software flow control.
Wait time	Wait time specifies the time that the CM or CB waits to receive CTS after asserting RTS, or for receiving an XON after receiving an XOFF, depending on the type of data flow control. If the wait time expires before the communication interface receives an expected CTS or XON, the CM or CB aborts the transmit operation and returns an error to the STEP 7 program. You specify the wait time in milliseconds. The range is 1 to 65535 milliseconds.

7.12.5.2 Managing flow control

Flow control refers to a mechanism for balancing the sending and receiving of data transmissions to avoid the loss of data. Flow control ensures that a transmitting device is not sending more information than a receiving device can handle. Flow control can be accomplished through either hardware or software. The RS232 mode of the CM 1241 RS232/422/485 module supports both hardware and software flow control. The RS422 mode of the CM 1241 RS232/422/485 module supports software flow control. You specify the type of flow control either when you configure the port or with the Port_Config instruction. The RS485 mode of the CM (1241 RS232/422/485) and the CB 1241 RS485 do not support flow control.

Hardware flow control works through the Request-to-send (RTS) and Clear-to-send (CTS) communication signals. For the RS232 mode of the CM 1241 RS232/422/485 module ([Page 491](#)), the RTS signal is output from pin 6 and the CTS signal is received through pin 5 of the X30 wiring terminal. The RS232 mode of the CM 1241 RS232/422/485 module is a DTE (Data Terminal Equipment) device which asserts RTS as an output and monitors CTS as an input.

Hardware flow control: RTS switched

If you enable RTS switched hardware flow control for the RS232 mode of the CM 1241 RS232/422/485, the module sets the RTS signal active to send data. The CM module monitors the CTS signal to determine whether the receiving device can accept data. When the CTS signal is active, the module can transmit data as long as the CTS signal remains active. If the CTS signal goes inactive, then the transmission must stop.

Transmission resumes when the CTS signal becomes active. If the CTS signal does not become active within the configured wait time, the module aborts the transmission and returns an error to the STEP 7 program. You specify the wait time in the port configuration ([Page 282](#)).

7.12 Point-to-point (PtP) communication

The RTS switched flow control is useful for devices that require a signal that the transmit is active. An example would be a radio modem that uses RTS as a "Key" signal to energize the radio transmitter. The RTS switched flow control will not function with standard telephone modems. Use the RTS always on selection for telephone modems.

Hardware flow control: RTS always on

In "RTS always ON" mode, the CM 1241 RS232/422/485 sets RTS active by default. A device acting as a communication partner monitors the RTS signal from the CM and utilizes this signal as a clear-to-send. The device only transmits to the CM when RTS is active, that is, when the device sees an active CTS. If RTS is inactive, the device does not transmit to the CM.

To allow the device to send data to the CM at any time, configure "RTS always ON" hardware flow control. The CM thus sets the RTS signal active all the time. The CM will not set RTS inactive even if the device cannot accept characters. The transmitting device must ensure that it does not overrun the receive buffer of the CM.

Data Terminal Ready (DTR) and Data Set Ready (DSR) signal utilization

The CM sets DTR active for either type of hardware flow control. The module transmits only when the DSR signal becomes active. The state of DSR is only evaluated at the start of the send operation. If DSR becomes inactive after transmission has started, the transmission will not be paused.

Software flow control

Software flow control uses special characters in the messages to provide flow control. You configure Hex characters that represent XON and XOFF.

XOFF indicates that a transmission must stop. XON indicates that a transmission can resume. XOFF and XON must not be the same character.

When the transmitting device receives an XOFF character from the receiving device, it stops transmitting. Transmitting resumes when the transmitting device receives an XON character. If it does not receive an XON character within the wait time that is specified in the port configuration [\(Page 282\)](#), the CM aborts the transmission and returns an error to the STEP 7 program.

Software flow control requires full-duplex communication, as the receiving partner must be able to send XOFF to the transmitting partner while a transmission is in progress. Software flow control is only possible with messages that contain only ASCII characters. Binary protocols cannot utilize software flow control.

7.12.5.3 Configuring transmit (send) and receive parameters

Before the CPU can engage in PtP Freeport communications, you must configure parameters for transmitting (or sending) messages and receiving messages. These parameters dictate how communications operate when messages are being transmitted to or received from a target device.

7.12.5.4 Configuring transmit (send) parameters

From the device configuration of the CPU, you configure how a communication interface transmits data by setting the "Configuration of message transfer" properties for the selected interface.

Configuration of message transfer

Frame default settings

☐ Send break before frame start

Break duration: 12 Bit times

☐ Send idle line

Duration of the idle line: 384 Bit times

RTS delay

RTS ON delay: 0 ms

RTS OFF delay: 0 ms

End delimiter

☐ Send up to and including end delimiter

No. of end delimiters: 0

1st end delimiter (Hex): 0

1st end delimiter (ASCII): NUL

2nd end delimiter (Hex): 0

2nd end delimiter (ASCII): NUL

Appended characters

Number of appended characters: 0

	Hex	ASCII
1	0	NUL
2	0	NUL
3	0	NUL
4	0	NUL
5	0	NUL

You can also dynamically configure or change the message transfer parameters from the STEP 7 program by using the Send_Config instruction ([Page 300](#)).

NOTE

Parameter values set from the Send_Config instruction in the STEP 7 program override the "Configuration of message transfer" properties. Note that the CPU does not retain parameters set from the Send_Config instruction in the event of power down or transition to STOP.

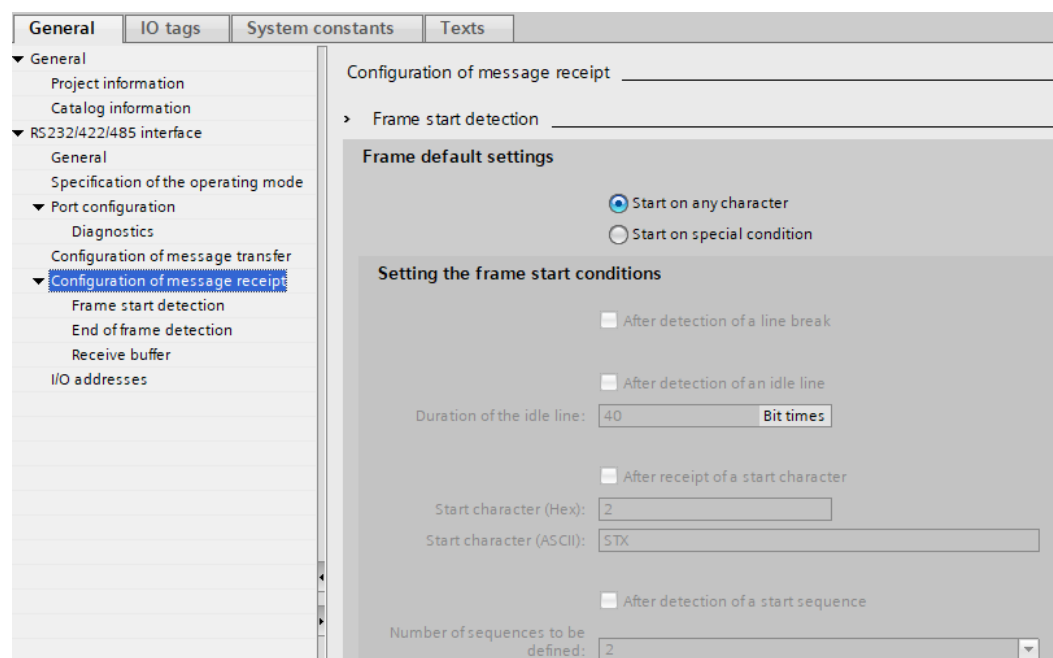
7.12 Point-to-point (PtP) communication

Parameter	Definition
Send break before frame start Break duration	Specifies that upon the start of each frame, a break will be sent after the RTS On delay (if configured) has expired and CTS is active. You specify how many bit times constitute a break where the line is held in a spacing condition. The default is 12 and the maximum is 65535, up to a limit of eight seconds.
Send idle line Duration of the idle line	Specifies that an idle line will be sent before message start. It is sent after the break, if a break is configured. The "Duration of the idle line" parameter specifies how many bit times constitute an idle line where the line is held in a marking condition. The default is 384 and the maximum is 65535, up to a limit of eight seconds.
RTS ON delay	Specifies the amount of time to wait after activating RTS before transmission is initiated. The range is 0 to 65535 ms, with a default value of 0. This parameter is valid only when the port configuration (Page 282) specifies hardware flow control. CTS is evaluated after the RTS On delay time has expired. This parameter is applicable for the RS232 mode of CM 1241 RS232/422/485 only.
RTS OFF delay	Specifies the amount of time to wait before deactivating RTS after completion of transmission. The range is 0 to 65535 ms, with a default value of 0. This parameter is valid only when the port configuration (Page 282) specifies hardware flow control. This parameter is applicable for RS232 mode of CM 1241 RS232/422/485 only.
Send up to and including end delimiter No. of end delimiters	You can configure the number of end delimiters (1 or 2) and their value. All data up to the end delimiter(s) is sent, independent of the selected frame length. The end delimiter must be included in the data to be sent. Data is sent only up to and including the delimiter, even if the specified data length is longer.
1st end delimiter (Hex) 1st end delimiter (ASCII)	Entry of the first end delimiter of a maximum of two end delimiters for the end criteria "Send up to and including end delimiter". The selected end delimiter or the selected end delimiter combination limits the length of the frame.
2nd end delimiter (Hex) 2nd end delimiter (ASCII)	Entry of the second end delimiter of a maximum of two end delimiters for the end criteria "Send up to and including end delimiter". The selected end delimiter combination limits the length of the frame.
Number of appended characters	Input of the number of appended characters. Sending takes place up to the configured length. The end delimiter(s) is/are appended automatically. Depending on the number of end delimiters, the CM sends one to five characters more than the number specified at the instruction to the partner.

7.12.5.5 Configuring receive parameters

The configuration options for a communication interface include settings for receiving data and recognizing the start and end of a message.

Set these parameters in the "Configuration of message receipt" properties for the selected interface.



You can also dynamically configure or change the receive message parameters from the STEP 7 program by using the Receive_Config instruction ([Page 300](#)).

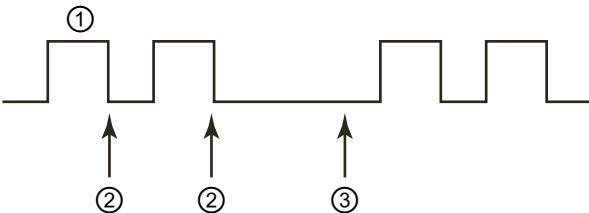
NOTE

Parameter values set from the Receive_Config instruction in the STEP 7 program override the "Receive message configuration" properties. Note that the CPU does not retain parameters set from the Receive_Config instruction in the event of power down or transition to STOP.

Frame start detection

You can determine how the communication interface recognizes the start of a message. The start characters and the characters comprising the message go into the receive buffer until a configured end condition is met.

You can specify multiple start conditions. If you specify more than one start condition, all of the start conditions must be met before the message is considered started. For example, if you configure an idle line time and a specific start character, the CM or CB will first look for the idle line time requirement to be met and then the CM or CB will look for the specified start character. If some other character is received (not the specified start character), the CM or CB will restart the start of message search by again looking for an idle line time.

Parameter	Definition
Start on any character	The "Start on any character" condition specifies that any successfully received character indicates the start of a message. This character is the first character within a message.
Start on special condition	The start of the message is detected based on the following specified conditions: • After detection of a line break • After detection of an idle line • After receipt of a start character • After receipt of a start sequence
Special condition: After detection of a line break	Specifies that a message receive operation starts after a break character is received.
Special condition: After detection of an idle line	Specifies that a message reception starts once the receive line has been idle or quiet for the number of specified bit times. Once this condition occurs, the start of a message begins.  ① Characters ② Restarts the idle line timer ③ Idle line is detected and message receive is started
Special condition: After receipt of a start character	Specifies that a particular character indicates the start of a message. This character is then the first character within a message. Any character that is received before this specific character is discarded. The default character is STX.
Special condition: After detection of a start sequence	Specifies that a particular character sequence from up to four configured sequences indicates the start of a message. For each sequence, you can specify up to five characters. For each character position, you specify either a specific hex character, or that the character is ignored in sequence matching (wildcard character). The last specific character of a character sequence terminates that start condition sequence. Incoming sequences are evaluated against the configured start conditions until a start condition has been satisfied. Once the start sequence has been satisfied, evaluation of end conditions begins. You can configure up to four specific character sequences. You use a multiple-sequence start condition when different sequences of characters can indicate the start of a message. If any one of the character sequences is matched, the message is started.

The communication interface checks start conditions in the following order:

- Idle line
- Broken line
- Character or character sequences

While checking for multiple start conditions, if one of the conditions is not met, the CM or CB restarts the checking with the first required condition. After the CM or CB establishes that the start conditions have been met, it begins evaluating end conditions.

Example configuration: Start message on one of two character sequences

Consider the following start message condition configuration:

Frame default settings

☐ Start on any character
☒ Start on special condition

Setting the frame start conditions

☐ After detection of a line break
☐ After detection of an idle line
 Duration of the idle line: 40 Bit times
☐ After receipt of a start character
 Start character (Hex): 2
 Start character (ASCII): STX
☒ After detection of a start sequence
 Number of sequences to be defined: 2

Frame start sequence 1

	Check this character	Character (HEX)	Character (ASCII)
1	☒	6A	j
2	☐	0	NUL
3	☐	0	NUL
4	☐	0	NUL
5	☒	1C	FS

Frame start sequence 2

	Check this character	Character (HEX)	Character (ASCII)
1	☐	0	NUL
2	☒	6A	j
3	☒	6A	j
4	☐	0	NUL
5	☐	0	NUL

With this configuration, the start condition is satisfied when either pattern occurs:

- When a five-character sequence is received where the first character is 0x6A and the fifth character is 0x1C. The characters at positions 2, 3, and 4 can be any character with this configuration. After the fifth character is received, evaluation of end conditions begins.
- When two consecutive 0x6A characters are received, preceded by any character. In this case, evaluation of end conditions begins after the second 0x6A is received (3 characters). The character preceding the first 0x6A is included in the start condition.

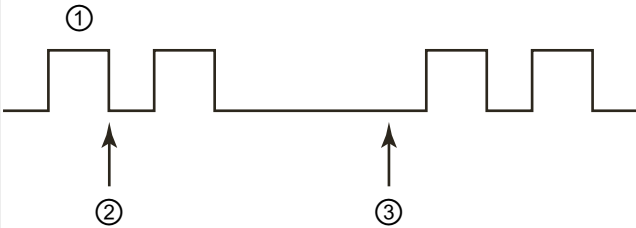
The following are example sequences that would satisfy this start condition:

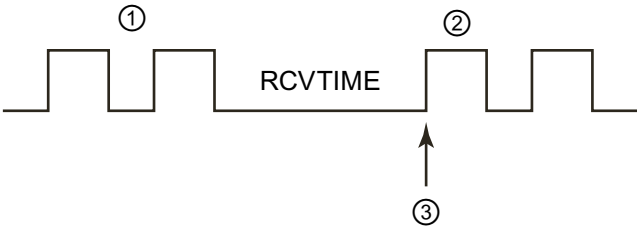
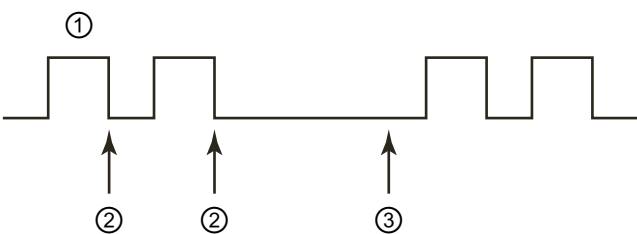
- <any character> 6A 6A
- 6A 12 14 18 1C
- 6A 44 A5 D2 1C

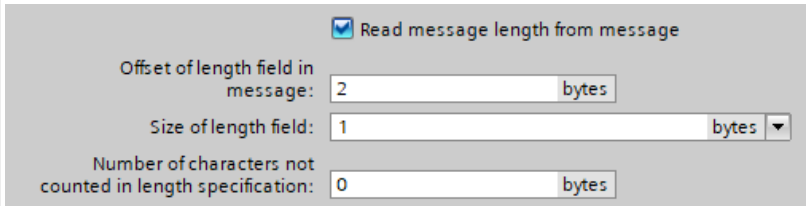
End of frame detection

You also configure how the communication interface recognizes the end of a message. You can configure multiple message end conditions. If any one of the configured conditions occurs, the message ends.

For example, you could specify an end condition with an end of message timeout of 300 milliseconds, an inter-character timeout of 40 bit times, and a maximum length of 50 bytes. The message ends if the message takes longer than 300 milliseconds to receive, or if the gap between any two characters exceeds 40 bit times, or if 50 bytes are received.

Parameter	Definition
Recognize message end by message timeout	The message end occurs when the configured amount of time to wait for the message end has expired. The message timeout period begins when a start condition has been satisfied. The default is 200 ms and the range is 1 to 65535 ms.  ① Received characters ② Start Message condition satisfied: message timer starts ③ Message timer expires and terminates the message

Parameter	Definition
Recognize message end by response timeout	The message end occurs when the configured amount of time to wait for a response expires before a valid start sequence is received. The response timeout period begins when a transmission ends and the CM or CB begins the receive operation. The default response timeout is 200 ms and the range is 1 to 65535 ms. If a character is not received within the response time period, RCVTIME, then an error is returned to the corresponding Receive_P2P instruction. The response timeout does not define a specific end condition. It only specifies that a character must be successfully received within the specified time. You must configure another end condition to indicate the actual end of a message.  ① Transmitted characters ② Received characters ③ First character must be successfully received by this time.
After character delay time elapses	The message end occurs when the maximum configured timeout between any two consecutive characters of a message has expired. The default value for the inter-character gap is 288 bit times and the maximum number is 65535 bit times, up to a maximum of eight seconds.  ① Received characters ② Restarts the intercharacter timer ③ The intercharacter timer expires and terminates the message.
After receipt of a fixed frame length	The message end occurs after a fixed frame length has been received. The valid range for the fixed length is 1 to 4096. The default is 1.
After receipt of a maximum number of characters	The message end occurs when the specified number of characters has been received. The valid range for the number of specified characters is 1 to 4096. the default is 1.
Read message length from message	The message specifies the length of the message. The message end occurs when a message of the specified length has been received. When you select the special condition where the message length is included in the message, you must provide three parameters that define information about the message length. The actual message structure varies according to the protocol in use. The three parameters are as follows: • Offset of length field in message: Set the character position (1-based) within the message that starts the length specifier. The valid range is 0-4095 with a default of 0 bytes. • Size of length field: Set the number of bytes (one, two, or four) of the length specifier. • Number of characters not counted in length specification: Set the number of characters following the length specifier that are not included in the length count. The valid range 0-255 with a default of 0 bytes.

Parameter	Definition
	The ending characters do not need to be contiguous. The "Number of characters not counted in length specification" value can be used to specify the length of a checksum field whose size is not included in the length field. 
After receipt of an end sequence	The message end occurs when a specified character sequence is received. You can specify a sequence of up to five characters. For each character position, you specify either a specific hex character, or that the character is ignored in sequence matching. Leading characters that are ignored characters are not part of the end condition. Trailing characters that are ignored characters are part of the end condition.

Example configuration: Read message length from message

Example 1: Consider a message structured according to the following protocol:

STX	Len (n)	Characters 3 to 14 counted by the length											
		ADR	PKE		INDEX		PWD		STW		HSW		BCC
1	2	3	4	5	6	7	8	9	10	11	12	13	14
STX	0x0C	xx	xxxx		xxxx		xxxx		xxxx		xxxx		xx

Configure the receive message length parameters for this message as follows:

- $n = 2$ (The message length starts with byte 2.)
- Length size = 1 (The message length is defined in one byte.)
- Length $m = 0$ (There are no additional characters following the length specifier that are not counted in the length count. Twelve characters follow the length specifier.)

In this example, the characters from 3 to 14 inclusive are the characters counted by Len (n).

Example 2: Consider another message structured according to the following protocol:

SD1	Len (n)	Len (n)	SD2	Characters 5 to 10 counted by length						FCS	ED
				DA	SA	FA	Data unit=3 bytes				
1	2	3	4	5	6	7	8	9	10	11	12
xx	0x06	0x06	xx	xx	xx	xx	xx	xx	xx	xx	xx

Configure the receive message length parameters for this message as follows:

- $n = 3$ (The message length starts at byte 3.)
- Length size = 1 (The message length is defined in one byte.)
- Length $m = 3$ (There are three characters following the length specifier that are not counted in the length. In the protocol of this example, the characters SD2, FCS, and ED are not counted in the length count. The other six characters are counted in the length count; therefore the total number of characters following the length specifier is nine.)

In this example, the characters from 5 to 10 inclusive are the characters counted by Len (n).

Example configuration: After receipt of an end sequence

Consider the following end message condition configuration:

	Check character 0	Character value (HEX):	Character (ASCII)
1	☐	0	NUL
2	☒	6A	j
3	☒	6A	j
4	☐	0	NUL
5	☐	0	NUL

In this case, the end condition is satisfied when two consecutive 0x6A characters are received, followed by any two characters. The character preceding the 0x6A 0x6A pattern is not part of the end character sequence. Two characters following the 0x6A 0x6A pattern are required to terminate the end character sequence. The values received at character positions 4 and 5 are irrelevant, but they must be received to satisfy the end condition.

NOTE

If you want your character sequence to indicate the end of the message, put the sequence in the last character positions. In the example above, if you wanted 0x6A 0x6A to end the message with no trailing characters, you would configure 0x6A in character positions 4 and 5.

7.12.6 3964(R) communication

The S7-1200 G2 CPU supports the 3964(R) protocol (RS232 or RS422 only) to enable communication between a CM 1241 RS232/422/485 and a communication partner that uses the 3964(R) protocol. Unlike PtP Freeport communication, where you define specific send (transmit) and receive characteristics for the messages, the 3964(R) protocol requires the following control characters:

- STX Start of text
Start of character string to be transmitted
- DLE Data Link Escape
Data transmission switchover
- ETX End of Text
End of character string to be transmitted
- BCC Block check character
- NAK Negative Acknowledge

Refer to the chapter describing serial data transmission principles in the S7-300 CP 341 Point-to-Point Communication, Installation, and Parameter Assignment Manual (<https://support.industry.siemens.com/cs/us/en/view/1117397>) for a complete description of the protocol.

Configuring the communication interface

To communicate to a partner using the 3964(R) protocol, you must include the CM 1241 RS232/422/485 (Page 491) in your device configuration in STEP 7. You then configure the communication ports (Page 282), priority, and protocol parameters (Page 299).

Communication to a partner with the 3964(R) protocol

When you configure a CM for 3964(R) protocol, you use the standard point-to-point send and receive instructions to transfer data between the CPU and its communication partner.

The CM embeds your data from the BUFFER parameter of the send instruction into the 3964(R) protocol and sends the data to the communication partner.

The CM receives data from the communication partner by means of the 3964(R) protocol, removes the protocol information, and returns the data in the BUFFER parameter of the receive instruction.

Refer to the following point-to-point instructions in the TIA Portal Information System:

- "Send P2P: Sending data (S7-1200, S7-1500)"
(https://docs.tia.siemens.cloud/access?ft:originId=. /39512235019/CM1500_Prog_Send_P2P_enUS.htm&ft:clusterId. /39512235019/CM1500_Prog_Send_P2P.htm)
- "Receive P2P: Receiving data (S7-1200, S7-1500)"
(https://docs.tia.siemens.cloud/access?ft:originId=. /39512235019/CM1500_Prog_Receive_P2P_enUS.htm&ft:clusterId. /39512235019/CM1500_Prog_Receive_P2P.htm)

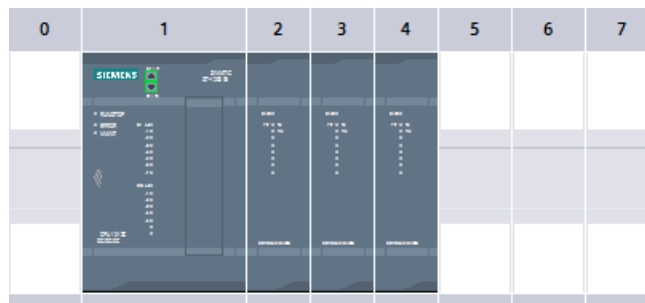
7.12.7 Configuring the 3964(R) communication

7.12.7.1 Configuring the 3964(R) communication ports

You can use either of the following methods to configure the communication interfaces for 3964(R) communication:

- Use the device configuration in STEP 7 to configure the port parameters. The CPU stores the device configuration settings and applies the settings after a power cycle.
- Use the Port_Config instruction to set the port parameters. The port settings set by the instructions are valid while the CPU is in RUN mode. The port settings revert to the device configuration settings after a power cycle.

After adding the communication interfaces to the device configuration ([Page 165](#)), you configure parameters for the communication interfaces by selecting one of the configured CMs.



The "Properties" tab of the inspector window displays the parameters of the selected CM. Select "Port configuration" to edit the following parameters:

- Protocol: 3964(R) with "Performance optimized for many short frames" optional
- Data transfer rate
- Parity
- Data bits
- Stop bits
- "Activate break detection" optional (RS232 only)

7.12 Point-to-point (PtP) communication

The screenshot shows the 'Port configuration' window for an RS232/422/485 interface. The 'General' tab is selected. Under 'Port configuration', the 'Protocol' is set to '3964(R)'. There is a checkbox for 'Performance optimized for many short frames' which is currently unchecked. Under 'Port parameters', the 'Data transfer rate' is set to '9600', 'Parity' is 'No parity', 'Data bits' is '8 bits per character', and 'Stop bits' is '1'. At the bottom, there is a checkbox for 'Activate break detection' which is also unchecked.

Table 7-11 Parameter definitions

Parameter	Definition
Protocol	3964R or Freeport/Modbus. Select 3964R to configure port for 3964(R) communication. Select the checkbox to optimize performance for many short frames.
Data transfer rate	The default value for the data transmission rate is 9600 bits/s. Valid choices in bits/s are: • 300 • 600 • 1200 • 2400 • 4800 • 9600 • 19200 • 38400 • 57600 • 76800 • 115200 • 250000 (RS422 only)
Parity	The default value for parity is no parity. Valid choices are: • No parity • Even parity • Odd parity • Mark (set parity bit to 1) • Space (set parity bit to 0)
Data bits	The number of data bits in a character. Valid choices are 7 or 8.
Stop bits	The number of stop bits can be either 1 or 2. The default is 1.
Activate break detection	Select the "Activate break detection" checkbox (RS232 only) to allow the CM to continuously monitor the communication line for any breaks or interruptions in the data transmission.

NOTE

Set the "Specification of the operating mode" for 3964R to one of the following two modes:

- RS232 mode
- Full duplex (RS422) 4-wire operation point to point

7.12.7.2 Configuring the 3964(R) priority and protocol parameters

You can use either of the following methods to configure the communication interfaces for 3964(R) communication:

- In the device configuration of the communication interface, click "3964(R) configuration" to set the priority and configure the protocol parameters. The CPU stores the device configuration settings and applies the settings after a power cycle.
- Use the P3964_Config instruction (Page 300) to set the priority and protocol configuration parameters. The values set by the instructions are valid while the CPU is in RUN mode. The values revert to the device configuration settings after a power cycle.

The "Properties" tab of the inspector window displays the parameters of the selected CM. Select "3964(R) configuration" to edit the parameters.

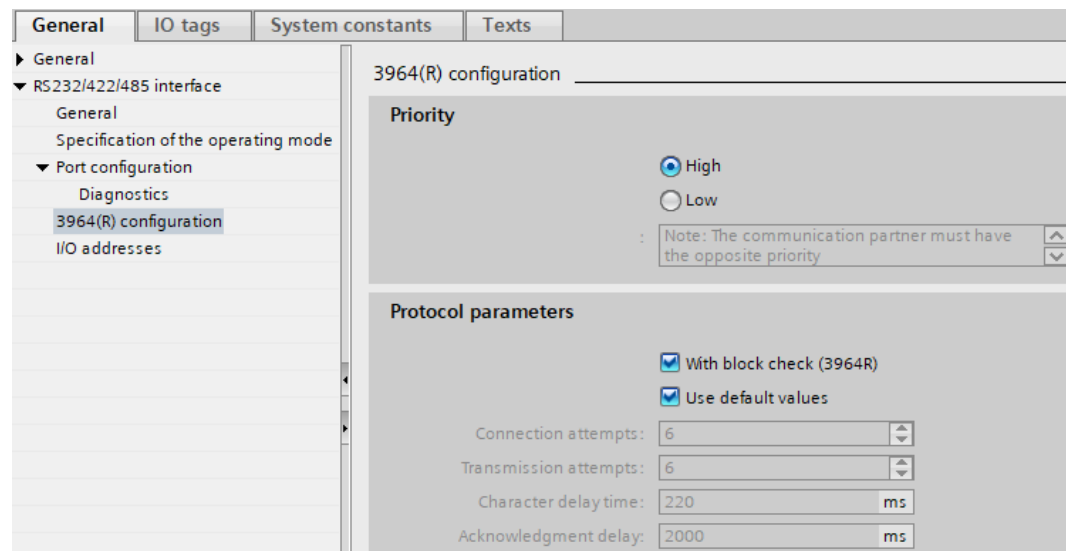


Table 7-12 Parameter definitions

Parameter	Definition
Priority	High or low: The CM will be either high or low and the communication partner must be the opposite.
With block check (3964R)	If selected, 3964(R) communication employs transmission security by including a block check character (BCC). If not selected transmission security does not include a block check character.
Use default values	If selected, 3964(R) uses default values for the following protocol parameters: • Connection attempts • Transmission attempts • Character delay time • Acknowledgement delay

7.12 Point-to-point (PtP) communication

Parameter	Definition
	If not selected, you can configure values for each of these parameters.
Connection attempts	Number of connection attempts (default value: 6 connection attempts) 1 to 255
Transmission attempts	Number of transmission attempts (default value: 6 transmission attempts) 1 to 255
Character delay time	Character delay time setting (depending on the set data transmission rate) (default value: 220 ms) 20 ms to 65535 ms
Acknowledgement delay	Acknowledgment delay time setting (depending on the set data transmission rate) (default value: 2000 ms when block check is enabled; 550 ms when block check is not enabled) 20 ms to 65535 ms

NOTE

With the exception of Priority, the protocol settings must be the same for the CM module and the communication partner.

7.12.8 Point-to-Point Instructions

The PtP instructions

(https://docs.tia.siemens.cloud/access?ft:originId=/.39512235019/39512235019_enUS.htm&ft:clusterId/39512235019/39512235019.htm) provide for communication using various network protocols and include the following folder:

Communication	
Name	Description
► S7 communication	
► Open user communication	
► Others	
▼ Communication processor	
▼ PtP Communication	
► Port_Config	Configure PtP communication port
► Send_Config	Configure PtP sender
► Receive_Config	Configure PtP recipient
► P3964_Config	Configure protocol
► Send_P2P	Send data
► Receive_P2P	Receive data
► Receive_Reset	Delete receive buffer
► Signal_Get	Read status
► Signal_Set	Set accompanying signals
► Get_Features	Get extended functions
► Set_Features	Set extended functions
► USS communication	
► MODBUS (RTU)	

NOTE**Choosing an instruction by PLC family**

If the TIA Portal Information System presents an instruction differently based on PLC family, follow the S7-1500 option for the instruction topic.

7.12.9 Programming the PtP communications

7.12.9.1 Programming overview

The Point-to-Point instructions (Page 300) fall into two categories:

- Configuration instructions
- Communication instructions

Configuration instructions

Before your STEP 7 program can engage in PtP communication, you must configure the communication interface port and the parameters for sending data and receiving data.

You can perform the port configuration and message configuration for each CM or CB through the device configuration or through these instructions in your STEP 7 program:

- Port_Config
- Send_Config
- Receive_Config
- P3964_Config

Communication instructions

The PtP communication instructions enable the STEP 7 program to send messages to and receive messages

(https://docs.tia.siemens.cloud/access?ft:originId=../15891429899/20448736523_enUS.htm&ft:clusterId/15891429899/20448736523.htm) from the communication interfaces.

All of the PtP functions operate asynchronously. The STEP 7 program can use a polling architecture to determine the status of transmissions and receptions. Send_P2P and Receive_P2P can execute concurrently. The communication modules and communication board buffer the transmit and receive messages as necessary up to a maximum buffer size of 1024 bytes.

CMs and CBs send messages to and receive messages from the actual point-to-point devices. The message protocol is in a buffer that is either received from or sent to a specific communication port. The buffer and port are parameters of the send and receive instructions:

- Send_P2P
- Receive_P2P

Additional instructions provide the capability to reset the receive buffer, and to get and set specific CM signals and features:

- Receive_Reset
- Signal_Get
- Signal_Set
- Get_Features
- Set_Features

7.12.9.2 Polling architecture

The STEP 7 program must call the point-to-point instructions cyclically or periodically to check for received messages. Polling the send cyclically or periodically determines when the transmit has completed.

Polling architecture: client

The typical sequence for a client is as follows:

1. A Send_P2P instruction initiates a transmission to the CM or CB.
2. The Send_P2P instruction executes on subsequent scans to poll for the transmit complete status.
3. When the Send_P2P instruction indicates that the transmission is complete, the STEP 7 program logic can prepare to receive the response.
4. The Receive_P2P instruction executes repeatedly to check for a response. When the CM or CB has collected a response message, the Receive_P2P instruction copies the response to the CPU and indicates that new data have been received.
5. The STEP 7 program can process the response.
6. Go to step 1 and repeat the cycle.

Polling architecture: server

The typical sequence for a server is as follows:

1. The STEP 7 program executes the Receive_P2P instruction every scan.
2. When the CM or CB has received a request, the Receive_P2P instruction indicates the availability of new data and the request is copied into the CPU.
3. The STEP 7 program services the request and generates a response.
4. Use a Send_P2P instruction to send the response back to the client.
5. Repeatedly execute Send_P2P to be sure the transmit occurs.
6. Go to step 1 and repeat the cycle.

The server must be responsible for calling Receive_P2P frequently enough to receive a transmission from the client before the client times out while waiting for a response. To accomplish this task, the STEP 7 program can call Receive_P2P from a cyclic OB, where the cycle time is sufficient to receive a transmission from the client before the timeout period expires. If you set the cycle time for the OB to provide for two executions within the timeout period of the client, the STEP 7 program can receive transmissions without missing any.

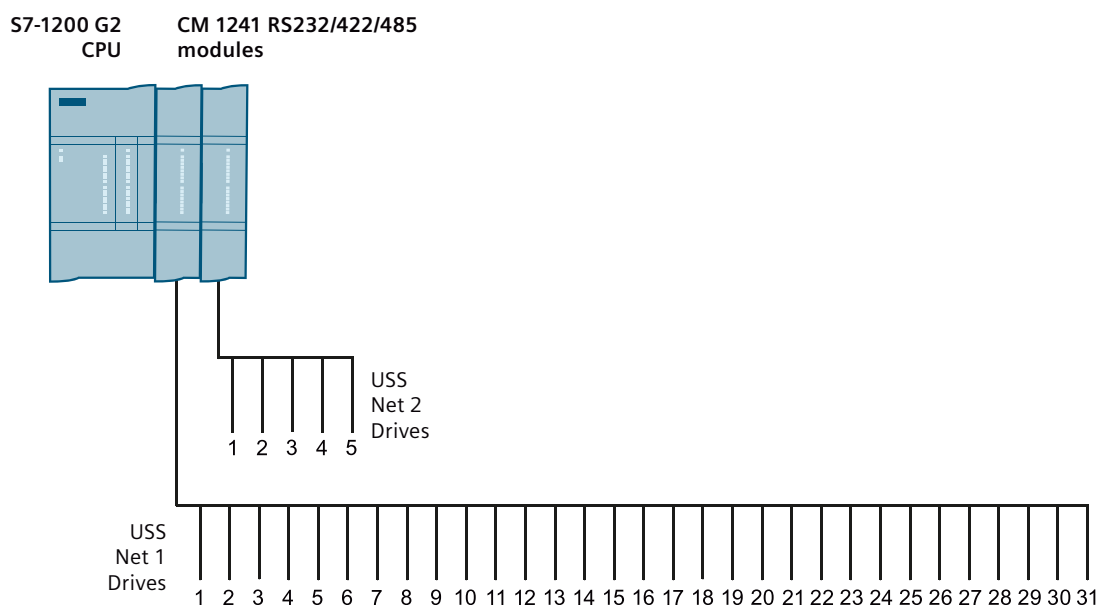
7.13 Universal serial interface (USS) communication

The USS instructions (Page 305) control the operation of motor drives which support the universal serial interface (USS) protocol. You can use the USS instructions to communicate with multiple drives through RS485 connections. Each RS485 port can operate up to 31 drives.

You can use the USS instructions to communicate with multiple drives through RS485 connections to CM 1241 RS232/422/485 communication modules or CB 1241 RS485 communication boards. The following CM/CB combinations can be installed:

- For 1212C and 1212FC CPUs, up to three CM 1241 RS232/422/485 modules and one CB 1241 RS485 for a total of four communication interfaces
- For 1214C and 1214FC CPUs, up to three CM 1241 RS232/422/485 modules and up to two CBs 1241 RS485 for a total of five communication interfaces

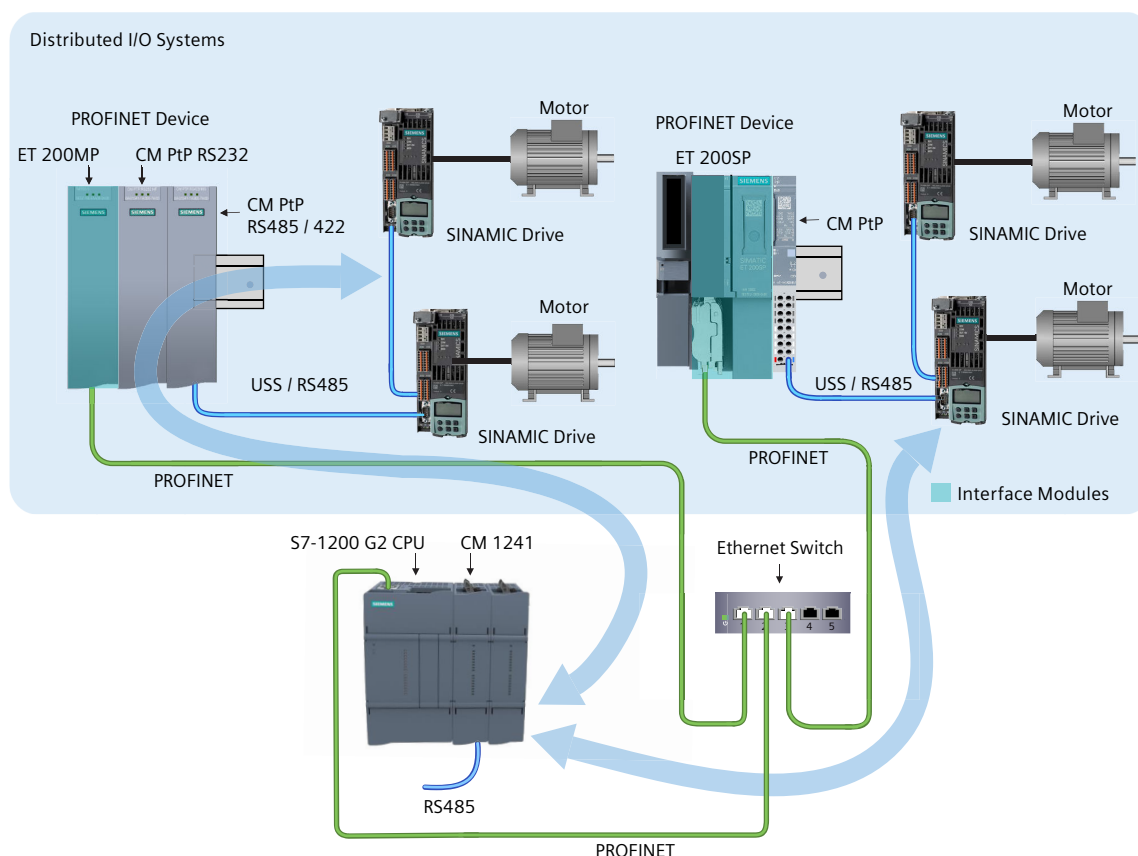
The USS protocol uses a master-slave network for communications over a serial bus. The master uses an address parameter to send a message to a selected slave. A slave itself can never transmit without first receiving a request to do so. Direct message transfer between the individual slaves is not possible. USS communication operates in half-duplex mode. The following USS illustration shows a network diagram for an example drive application.



USS communications through PROFINET

USS communication enables you to use a PROFINET distributed I/O rack to communicate to various devices (RFID readers, GPS device, and others). You connect the Ethernet interface of the S7 1200 G2 CPU to a PROFINET interface module. PtP communication modules in the rack with the interface module provide serial communications to USS drives.

USS instructions allow you to configure the communications between the PtP communication modules in the distributed I/O rack and the USS drives.



The blue arrows indicate the flow of bidirectional communication between devices.

Note that STEP 7 provides different versions

(https://docs.tia.siemens.cloud/access?ft:originId=/.75629918475/95949438091_enUS.htm&ft:clusterId=/.75629918475/95949438091.htm) of the USS instructions (Page 305) depending on the number of drives.

Requirements for using the USS protocol

The USS communication instructions support the USS protocol with usage requirements (https://docs.tia.siemens.cloud/access?ft:originId=/.39512292235/40514327819_enUS.htm&ft:clusterId=/.39512292235/40514327819.htm). For each USS network, one instance data block (DB) is used for USS_Port_Scan and one instance data block for all calls of USS_Drive_Control.

7.13.1 USS instructions

USS instructions

(https://docs.tia.siemens.cloud/access?ft:originId=../39512292235/39512292235_enUS.htm&ft:clusterId/39512292235/39512292235.htm) provide for communication using various network protocols and include the following folder groups:

Communication	
Name	Description
▸ S7 communication	
▸ Open user communication	
▸ Others	
▾ Communication processor	
▸ PtP Communication	
▾ USS communication	
▣ USS_Port_Scan	Communication via USS network
▣ USS_Drive_Control	Data exchange with the drive
▣ USS_Read_Param	Read data from drive
▣ USS_Write_Param	Change data in drive
▣ USS_Port_Scan_31	Communication via USS network for 31 slaves
▣ USS_Drive_Control_31	Data exchange with the drive for 31 slaves
▣ USS_Read_Param_31	Read data from the drive for 31 slaves
▣ USS_Write_Param_31	Change data in the drive for 31 slaves
▸ MODBUS (RTU)	

The following instructions operate a maximum of 16 USS drives:

- USS_Port_Scan
- USS_Drive_Control
- USS_Read_Param
- USS_Write_Param

The following instructions operate a maximum of 31 USS drives:

- USS_Port_Scan_31
- USS_Drive_Control_31
- USS_Read_Param_31
- USS_Write_Param_31

NOTE

Choosing an instruction by PLC family

If the TIA Portal Information System presents an instruction differently based on PLC family, follow the S7-1500 option for the instruction topic.

7.13.2 USS status codes

The STATUS output of the USS functions returns the USS instruction status codes.

Table 7-13 STATUS codes ¹

STATUS (W#16#....)	Description
0000	No error
8180	The length of the drive response did not match the characters received from the drive. The drive number where the error occurred is returned in the "USS_Extended_Error" variable. See the extended error description below this table.
8181	VALUE parameter was not a Word, Real or DWord data type.
8182	The instruction supplied a Word for a parameter value and received a DWord or Real from the drive in the response.
8183	The instruction supplied a DWord or Real for a parameter value and received a Word from the drive in the response.
8184	The response telegram from drive had a bad checksum. The drive number where the error occurred is returned in the "USS_Extended_Error" variable. See the extended error description below this table.
8185	Illegal drive address. Valid drive address range: 1 to16 (or 1-31 if using the _31 instructions).
8186	The speed set point is out of the valid range (valid speed SP range: -200% to 200%).
8187	The wrong drive number responded to the request sent. The drive number where the error occurred is returned in the "USS_Extended_Error" variable. See the extended error description below this table.
8188	Illegal Programmable Zero Delay (PZD) word length specified (valid range = 2, 4, 6 or 8 words).
8189	Illegal Baud Rate was specified.
818A	The parameter request channel is in use by another request for this drive.
818B	The drive has not responded to requests and retries. The drive number where the error occurred is returned in the "USS_Extended_Error" variable. See the extended error description below this table.
818C	The drive returned an extended error on a parameter request operation. See the extended error description below this table.
818D	The drive returned an illegal access error on a parameter request operation. See your drive manual for information of why parameter access may be limited.
818E	The drive has not been initialized. This error code is returned to USS_Read_Param or USS_Write_Param when USS_Drive_Control, for that drive, has not been called at least once. This keeps the initialization on first scan of USS_Drive_Control from overwriting a pending parameter read or write request, since it initializes the drive as a new entry. To fix this error, call USS_Drive_Control for this drive number.
8280	Negative acknowledgment when reading module.
8281	Negative acknowledgment when writing module.
8FFF	The module is not ready temporarily due to a reset.
80Ax-80Fx	Specific errors returned from PtP communication instructions called by the USS Library - These error code values are not modified by the USS library and are defined in the PtP instruction descriptions.

¹ In addition to the USS instruction errors listed above, errors can be returned from the underlying PtP communication instructions.

For several STATUS codes, additional information is provided in the USS_Extended_Error variable of the USS_Drive_Control Instance DB. For STATUS codes hexadecimal 8180, 8184, 8187, and 818B, USS_Extended_Error contains the drive number where the communication error occurred. For STATUS code hexadecimal 818C, USS_Extended_Error contains a drive error code returned from the drive when using a USS_Read_Param or USS_Write_Param instruction.

Read and write access to a drive's internal parameters

USS drives support read and write access to a drive's internal parameters. This feature allows remote control and configuration of the drive. Drive parameter access operations can fail due to errors such as values out of range or illegal requests for a drive's current mode. The drive generates an error code value that is returned in the USS_Extended_Error variable when the STATUS code value is hexadecimal 818C. This error code value is only valid for the last execution of a USS_Read_Param or USS_Write_Param instruction. The error code value of USS_Extended_Error depends on the drive model. See the drive's manual for a description of the extended error codes for read and write parameter operations.

7.13.3 USS general drive setup requirements

USS general drive setup requirements consist of the following points:

- The drives must be set to use 4 Parameter Control Words (PKW).
- The drives can be configured for 2, 4, 6, or 8 Programmable Zero Delay (PZD) words.
- The number of PZD words in the drive must match PZD_LEN input on the USS_Drive_Control instruction for that drive.
- The baud rate in all the drives must match the BAUD input on the USS_Port_Scan instruction.
- The drive must be set for remote control.
- The drive must be set for frequency set-point to USS on COM Link.
- The drive address must be set to 1 to 16 (or 1-31 if using the _31 instructions) and match the DRIVE input on the USS_Drive_Control block for that drive.
- The drive direction control must be set to use the polarity of the drive set-point.
- The RS485 network must be terminated properly.

7.14 Modbus communication

Modbus function codes

A CPU operating as a Modbus TCP client or Modbus RTU master can read/write both data and I/O states in a remote Modbus TCP server or Modbus RTU slave. Remote data can be read and then processed in your program logic.

A CPU operating as a Modbus TCP server or Modbus RTU slave allows a supervisory device to read/write both data and I/O states in CPU memory. A Modbus TCP client or Modbus RTU master can write new values into server/slave CPU memory that is available to your program logic.

WARNING

Avoiding security risks from network attacks

If an attacker can access your networks, the attacker can possibly read and write data.

For example, I/O exchange through PROFINET, PUT/GET (Page 267), T-Block, and communication modules (CMs) have no security features. You must protect these forms of communication.

If you fail to protect these forms of communication, death or severe personal injury can result.

For security information and recommendations, see the "Operational Guidelines (<https://www.siemens.com/global/en/products/services/cert/news/operational-guidelines-for-industrial-security.html>)" white paper on the Siemens Industrial Cybersecurity Web site.

Table 7-14 Read data functions: Read remote I/O and program data

Modbus function code	Read slave (server) functions - standard addressing
01	Read output bits: 1 to 2000 bits per request
02	Read input bits: 1 to 2000 bits per request
03	Read holding registers: 1 to 125 words per request
04	Read input words: 1 to 125 words per request

Table 7-15 Write data functions: Write remote I/O and modify program data

Modbus function code	Write slave (server) functions - standard addressing
05	Write one output bit: 1 bit per request
06	Write one holding register: 1 word per request
15	Write one or more output bits: 1 to 1968 bits per request
16	Write one or more holding registers: 1 to 123 words per request

Modbus function codes 08 and 11 provide slave device communication diagnostic information.

Modbus function code 0 broadcasts a message to all slaves (with no slave response). The broadcast function is not available for Modbus TCP, because communication is connection based.

Modbus function code 23 can write and read one or more holding registers: 1 to 121/125 (Write/Read) words per request. This function code is only available for Modbus TCP.

Modbus network station addresses

In a Modbus TCP network, each device is uniquely addressed using its IP address and port number. To establish a connection, enter these details into the appropriate configuration field. The Modbus protocol then uses this address information to access and communicate with devices over the network.

Table 7-16 Modbus memory addresses

Station		Address range
TCP station	Station address	IP address and port number
RTU station	Standard station address	1 to 247
	Extended station address	1 to 65535

Modbus memory addresses

The actual number of available Modbus memory addresses depends on the CPU model, how much work memory exists, and how much CPU memory is used by other program data. The table below gives the nominal value of the address range.

Table 7-17 Modbus memory addresses

Station		Address range
TCP station	Standard memory address	10K
	Extended memory address	64K
RTU station	Standard memory address	10K
	Extended memory address	64K

7.14.1 Modbus TCP

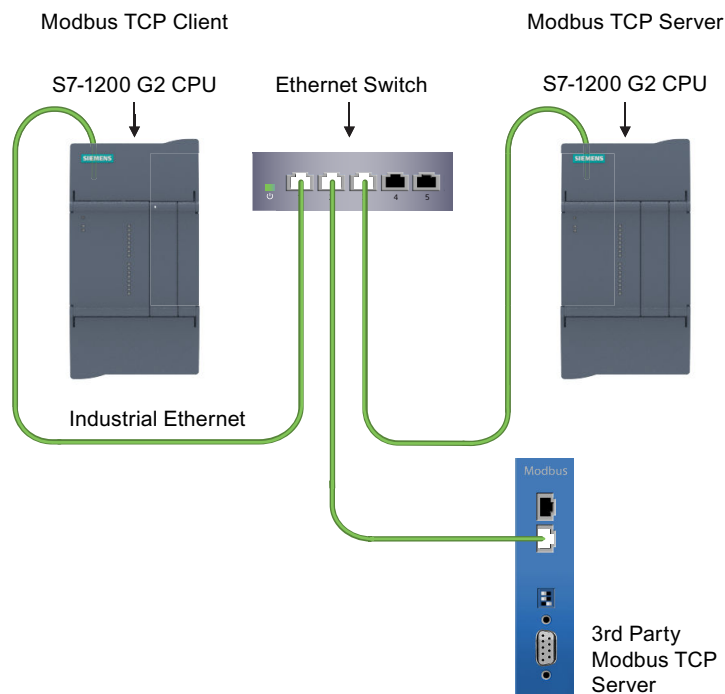
Modbus TCP (Transmission Control Protocol) is a standard network communication protocol that uses the PROFINET connector on the CPU for TCP/IP communication.

Modbus TCP uses Open User Communication (OUC) connections as a Modbus communication path. Multiple client-server connections can exist in addition to the connection between STEP 7 and the CPU. Mixed client and server connections are supported up to the maximum number of connections allowed by the CPU model ([Page 218](#)).

Each MB_SERVER connection must use a unique instance DB and port number. Only one connection per port number is supported. Each MB_SERVER (with its unique instance DB, IP address, and port number) must be executed individually for each connection.

A Modbus TCP client must control the client-server connection with the DISCONNECT parameter. The basic Modbus client actions are shown below:

1. Initiate a connection to a particular server IP address and port number.
2. Initiate client transmission of a Modbus message and receive the server responses.
3. Initiate the disconnection of client and server to enable connection with a different server.



7.14.1.1 Modbus TCP Instructions

The Modbus TCP instructions (https://docs.tia.siemens.cloud/access?ft:originId=/.30931262347/53718390539_enUS.htm&ft:clusterId=/.30931262347/53718390539.htm) provide the capability to communicate between Modbus TCP clients, Modbus TCP servers, and third-party Modbus TCP devices through a switch. These can be found in the following folders:

Communication	
Name	Description
▶ S7 communication	
▶ Open user communication	
▼ Others	
▼ MODBUS TCP	
■ MB_CLIENT	Communicate via PROFINET as Modbus TCP client
■ MB_SERVER	Communicate via PROFINET as Modbus TCP server
▶ Communication processor	

NOTE

Choosing an instruction by PLC family

If the TIA Portal Information System presents an instruction differently based on PLC family and "S7-1200 G2" is not an option , follow the S7-1500 option for the instruction topic.

Modbus TCP Redundancy instructions

The Modbus TCP Redundancy instructions (https://docs.tia.siemens.cloud/access?ft:originId=../30931262347/104082829707_enUS.htm&ft:clusterId./30931262347/104082829707.htm) provide the capability to ensure continuous and reliable communication between devices even in the event of a network or device failure. These can be found in the following folders:

Communication	
Name	Description
▸ S7 communication	
▸ Open user communication	
▸ OPC UA	
▾ Others	
▸ MODBUS TCP	
▾ MODBUS TCP Redundancy	
MB_RED_CLIENT	Redundant communication via PROFINET as Modbus TCP client
MB_RED_SERVER	Redundant communication via PROFINET as Modbus TCP server
▸ Communication processor	

NOTE

Choosing an instruction by PLC family

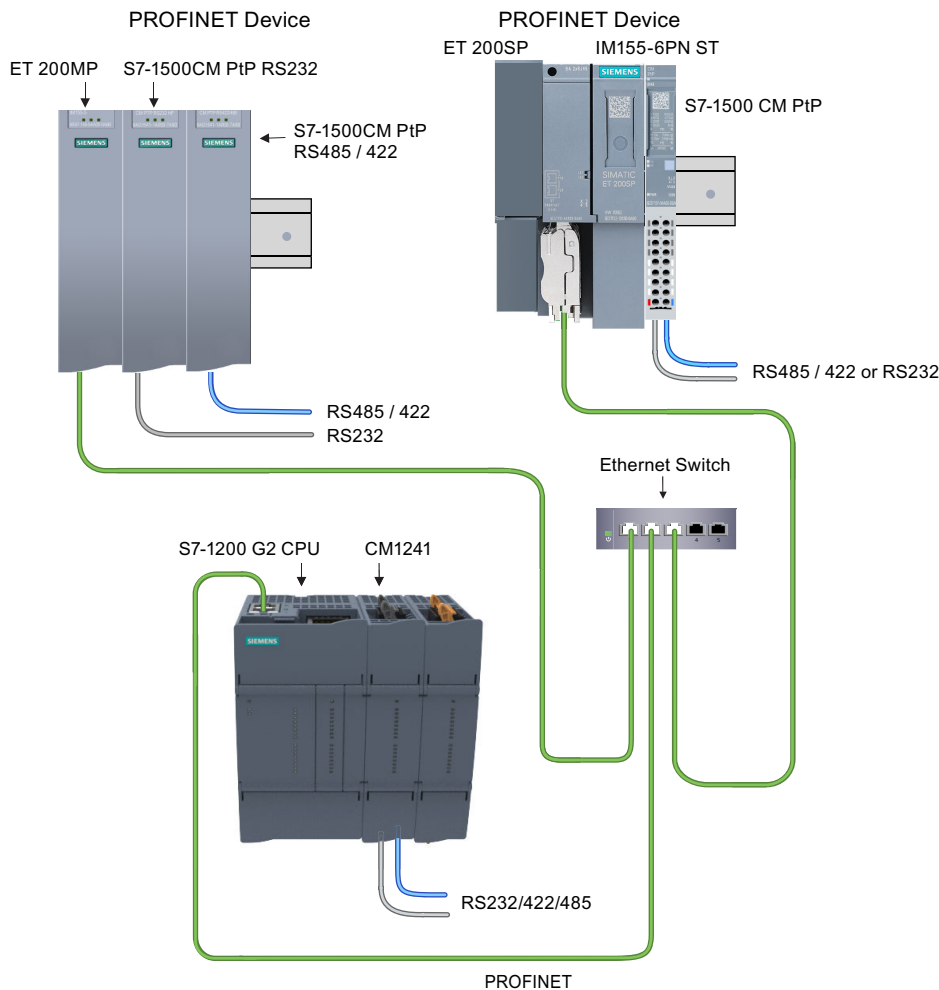
If the TIA Portal Information System presents an instruction differently based on PLC family and "S7-1200 G2" is not an option, follow the S7-1500 option for the instruction topic.

7.14.2 Modbus RTU

Modbus RTU (Remote Terminal Unit) is a standard network communication protocol that uses the RS232, RS422, or RS485 electrical connection for serial data transfer between Modbus network devices. You can add PtP (Point to Point) network ports to a CPU with a CM 1241 RS232/422/485 or a CB 1241 RS485.

Modbus RTU uses a master/slave network where all communications are initiated by a single Master device and slaves can only respond to a master's request. The master sends a request to one slave address and only that slave address responds to the command.

Modbus RTU enables you to use PROFINET distributed I/O to communicate to various devices (RFID readers, GPS device, and others). You connect the Ethernet interface of the S7-1200 G2 CPU to a PROFINET interface module. PtP communication modules in the rack with the interface module can then provide serial communications to external Modbus devices.



Modbus RTU communications hardware compatibility

The following table outlines the Modbus RTU protocol along with the available instruction set and communication hardware options for the protocol.

Protocol	Instruction Folder	Local CM 1241 RS232/422/485	Local CB 1241 RS485	Distributed CM PtP (example: ET 200MP CM or ET 200SP CM)
Modbus RTU	Communication > Communication processor > MODBUS (RTU)	Yes	Yes	Yes

7.14.2.1 Modbus RTU instructions and versions

The Modbus RTU instructions provide the ability to communicate between PtP communication modules or boards and Modbus devices in the network using RS232, RS422, or RS485.

Communication	
Name	Description
▸ S7 communication	
▸ Open user communication	
▸ Others	
▾ Communication processor	
▸ PtP Communication	
▸ USS communication	
▾ MODBUS (RTU)	
▣ Modbus_Comm_Load	Configure port for Modbus
▣ Modbus_Master	Communicate as Modbus master
▣ Modbus_Slave	Communicate as Modbus slave

For more information on the Modbus RTU instructions and their uses, see the following topics in the TIA Portal Information System:

- "Modbus Comm Load: Configure communication module for Modbus"
(https://docs.tia.siemens.cloud/access?ft:originId=./39512297483/CM1500_Prog_Modbus_Comm_Load_enUS.htm&ft:clusterId./39512297483/CM1500_Prog_Modbus_Comm_Load.htm)
- "Modbus Master: Communicate as Modbus master"
(https://docs.tia.siemens.cloud/access?ft:originId=./39512297483/CM1500_Prog_Modbus_Master_enUS.htm&ft:clusterId./39512297483/CM1500_Prog_Modbus_Master.htm)
- "Modbus Slave: Communicate as Modbus slave"
(https://docs.tia.siemens.cloud/access?ft:originId=./39512297483/CM1500_Prog_Modbus_Slave_enUS.htm&ft:clusterId./39512297483/CM1500_Prog_Modbus_Slave.htm)

NOTE

STEP 7 provides different library versions of the Modbus RTU instructions. For correct information on S7-1200 G2 Modbus RTU instruction library versions, refer to "Dependencies between library versions

(https://docs.tia.siemens.cloud/access?ft:originId=./39512297483/127801431179_enUS.htm&ft:clusterId./39512297483/127801431179.htm)" in the TIA Portal Information System.

NOTE**Choosing an instruction by PLC family**

If the TIA Portal Information System presents an instruction differently based on PLC family and "S7-1200 G2" is not an option, follow the S7-1500 option for the instruction topic.

7.14.2.2 Maximum number of supported Modbus slaves

Modbus addressing supports a maximum of 247 slaves (slave numbers 1 through 247). Each Modbus network segment can have a maximum of 32 devices, based upon the loading and drive capabilities of the RS485 interface. When you reach the 32-device limit, you must use a repeater to expand to the next segment. You need seven repeaters to support the 247 slaves connected to one master for RS485.

You cannot use Siemens repeaters with PROFINET. You require third party repeaters for Modbus.

Modbus timeouts are long by default; the use of multiple repeaters does not create a time-delay problem. Response delays do not affect the Modbus master.

Near Field Communication (NFC)

The S7-1200 G2 CPUs are equipped with embedded Near Field Communication (NFC) tags. This allows you to scan the passive tag in your CPU and access information via the S7-1200 G2 NFC application (app) from a smartphone device.

By default, NFC is disabled in a new STEP 7 project. If you want to use NFC in your STEP 7 project, you must enable it in the project before downloading the project to your CPU.

NOTE

if you disable NFC in your STEP 7 project and perform a new download to the CPU, the CPU clears the data on the NFC tag.

Installing the S7-1200 G2 NFC app on your smartphone device allows you to read information from the CPU.

For more information on using the Near Field Communication feature with S7-1200 G2, see the Near Field Communication (NFC) Function Manual

(<https://support.industry.siemens.com/cs/ww/en/view/109994538>).

WARNING

Risks when using a cellular phone in close proximity to the S7-1200 G2 CPU

Using a cellular phone in close proximity to the S7-1200 G2 system with cellular and Wi-Fi communications active could cause unpredictable behavior.

To reduce any influence of a cellular phone on the S7-1200 G2 system, and to ensure proper operation of your CPU, place the phone in "Airplane mode" to disable cellular and Wi-Fi before bringing the phone into proximity (<10 cm) of the CPU.

Failure to comply with these guidelines can cause damage or unpredictable operation which could result in severe personal injury, property damage, and/or death.

WARNING

Risks when operating a cellular phone in a hazardous or explosive environment

Do not use a cellular phone in a hazardous or explosive environment unless the phone has been approved for use in such environments.

Failure to comply with these guidelines can cause damage or unpredictable operation which could result in death or severe personal injury and/or property damage.

Web server

The S7-1200 G2 CPU Web server provides system Web pages

(https://docs.tia.siemens.cloud/r/simatic_s7_1500_et_200mp_manual_collection_enus_20/comprehensive-information/cpu-function-manuals/web-server/system-web-pages) and a Web API (https://docs.tia.siemens.cloud/r/simatic_s7_1500_et_200mp_manual_collection_enus_20/comprehensive-information/cpu-function-manuals/web-server/api-application-programming-interface/web-api) for you to develop custom Web pages that can read and write process data.

Your STEP 7 project enables system Web pages by default. You can find or change this setting from Web applications in the project tree.

Differences from the S7-1500 Web server

The S7-1200 G2 Web server implements the functionality of the S7-1500 Web server, with the following difference: The number of concurrent API sessions is 30.

Default page for Web application

You can set a default page from STEP 7 from Web applications in the project tree.

You can also use the following methods to set a default page for Web pages that you create with the Web API:

- `WebServer.SetDefaultPage`
- `WebApp.SetDefaultPage`

If you have not created a Web application and configured a default page, the Web browser returns a 404 error. For information on configuring and setting default pages, refer to the Web server manual

(https://docs.tia.siemens.cloud/r/simatic_s7_1500_et_200mp_manual_collection_enus_20/comprehensive-information/cpu-function-manuals/web-server). Use the Edition dropdown menu to select the correct version of the manual.

Examples

Refer to the online examples

(<https://support.industry.siemens.com/cs/ww/en/view/68011496>) for developing Web pages. The examples demonstrate a variety of functions.

Additional information

With the functionality of the Web API, S7-1200 G2 does not support the former AWP commands for developing user-defined Web pages.

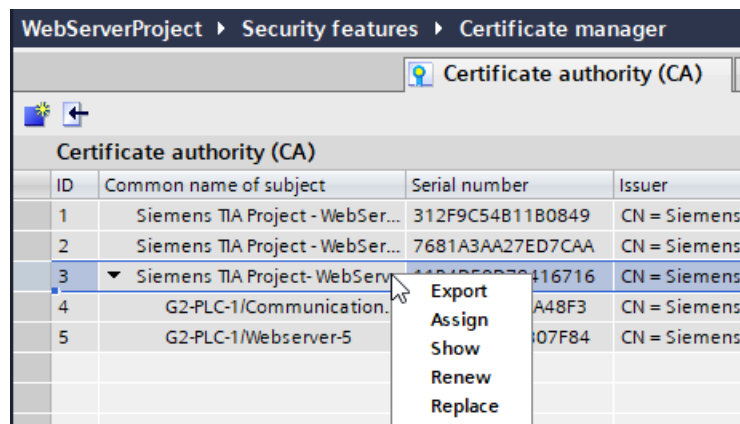
The Web API does not include a method for updating firmware.

9.1 Certificate requirements for the Web server

To communicate with the S7-1200 G2 Web API using a web browser, you must have a trusted Certificate Authority (CA) installed on your programming device. The trusted Certificate Authority (CA) enables secure communications over HTTPs.

The process includes the following tasks:

- Protecting the TIA Portal project from Security settings > Settings > Protect this project, as described in the TIA Portal Information System, Activating project protection topic
- Selecting "Use global security settings for certificate manager" for your CPU in the device configuration properties, Protection & Security > Certificate manager
- Creating a PLC communication certificate (Page 220)
- Enabling the Web server in the device configuration of the CPU (Page 166)
- Using the Security settings > Security features > Certificate manager to install or export the PLC communication certificate and Web server certificate, as described in the TIA Portal Information System, Certificate manager chapter



- Following the FAQ (<https://support.industry.siemens.com/cs/ww/en/view/103528224>) beginning with Step 2 to install, store, and trust the certificates you installed or exported from the TIA Portal project.

References

For additional information on managing certificates for the Web server, refer to the TIA Portal Information System and these documents:

- Web server manual (<https://support.industry.siemens.com/cs/ww/en/view/59193560>)
- How to install a certificate for the Web server (<https://support.industry.siemens.com/cs/ww/en/view/103528224>)

These documents are applicable to S7-1500 CPUs, but most of the content is applicable to S7-1200 G2 CPUs.

Motion control

10.1 Introducing S7-1200 G2 Motion Control

Motion Control allows users to accomplish specific tasks that require movement of tools or materials, such as bottling, machining, or welding.

Machines and production lines must increasingly be adapted to different formats, sizes, product types, and production processes. S7-1200 G2 Motion Control offers a precise, dynamic, and easy-to-implement solution.

Motion Control instructions control drives with PROFIdrive capability, drives with analog setpoint interface, servo motors, and stepper motors in accordance with the PLCopen standard. The axis control panel and comprehensive online and diagnostic functions support commissioning and optimization of drives. S7-1200 G2 Motion Control is fully integrated into the S7-1200 G2 CPU.

Achieving motion control

You can achieve Motion Control with the S7-1200 G2 CPU using the following concepts:

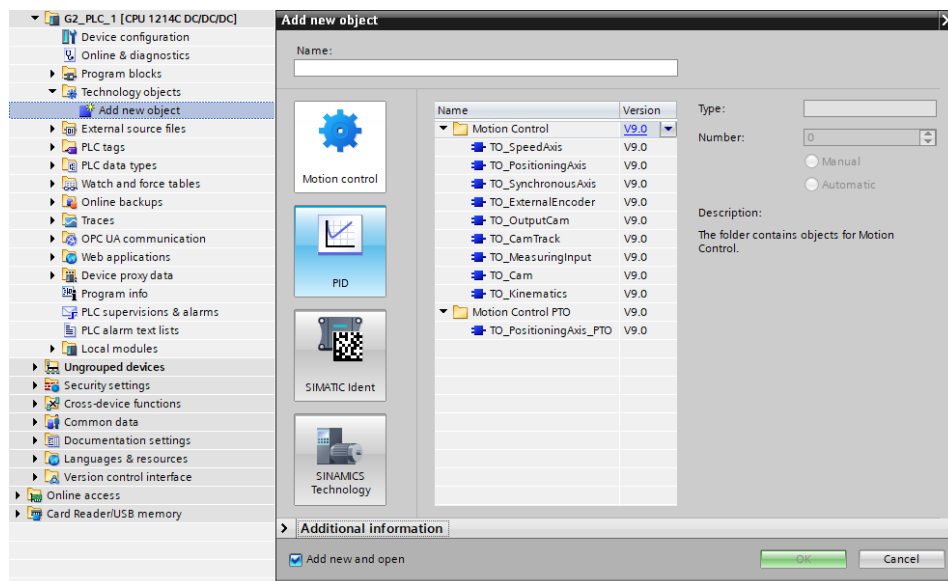
- Technology Objects serve as links to the drive and allow for configuration of dynamic behavior.
- Motion Control instructions allow you to control each Technology Object.
- Organization Blocks execute the Motion Control instructions of the user program in a structured manner.

10.2 Motion Control Technology Objects (TOs)

In S7-1200 G2 Motion Control, the technology objects (TO) represent control elements of Motion Control, such as a position axis or an output cam. A TO establishes a logical relationship between the user program and the physical device and defines the motion profile by allowing for parameterization, such as setting limits like acceleration, deceleration, and jerk. This information is stored in a corresponding technology data block (DB), where you can read information about the status of the motion control job, such as speed, position, or error status.

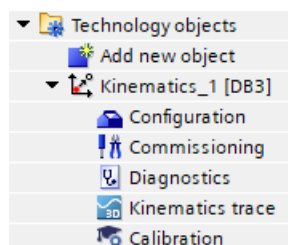
Creating a new TO

You can add a TO to your STEP 7 project by selecting "Add new object" under the Technology objects folder in the project tree.



Configuration and commissioning

Within STEP 7, multiple tools exist to help configure, commission, and debug TOs in your motion control project.



Motion resources

When you create a motion control TO, that TO draws from a pool of resources that represents the resources available within the CPU for motion tasks. There are two pools, one each for Motion Control and Extended Motion Control. If you exceed the number of resources available from either pool, an error occurs when you compile your program in the TIA Portal.

You can add up to 16 Pulse Train Output (PTO) TOs, which are independent of all other types of TOs. The PTO TOs do not draw from either pool of Motion Control resources.

The costs associated with each TO are additive in some cases. For example, implementing a three-axis Cartesian Portal solution requires one Kinematics TO, costing 30 Extended Motion Control resources, and three PositioningAxis TOs, costing 80 Motion Control resources each. In this case, the total cost is 30 Extended resources and 240 Motion resources.

You can find more information about motion resources in the Technical Specifications ([Page 356](#)).

NOTE

While S7-1200 CPUs allow for the sharing of a single PTO output between two configured positioning axes, this functionality might not function as intended in S7-1200 G2 projects. The first configured positioning axis behaves as expected, but the second configured positioning axis does not move.

Supported TOs

The S7-1200 G2 CPU provides varying levels of support for a range of Motion Control TOs, as described in the table below:

TO	Supported	Motion Control resources required (out of 800 provided by the CPU)	Extended Motion Control resources required (out of 40 provided by the CPU)
TO_SpeedAxis	✓	40	
TO_PositioningAxis	✓	80	
TO_SynchronousAxis	✓	160	
TO_ExternalEncoder	✓	80	
TO_OutputCam	✓	20	
TO_CamTrack	✓	160	
TO_MeasuringInput	✓	40	
TO_Cam	✓		2
TO_Kinematics	Partially supported		30
TO_PositioningAxis_PTO	✓	0	0

You can find help on programming each Motion Control TO in the TIA Portal Information System, as defined for the S7-1500/S7-1500T. These TOs are equivalent in S7-1200 G2.

10.3 Motion Control instructions

The STEP 7 program calls the Motion Control (MC) instructions and acts upon configured TOs. These blocks exist within the motion library as function blocks (FB) and create a data instance when they are placed into the user program in STEP 7.

You can use MC instructions to accomplish motion tasks of varying complexity, such as setting a constant velocity, moving a tool to a desired position, or synchronizing two axes.

Supported instructions

The following MC instructions are available for the S7-1200 G2 CPU:

MC instruction	Motion Control	Extended Motion Control	PTO Motion Control
MC_Power	✓		
MC_Reset	✓		
MC_Home	✓		
MC_Halt	✓		
MC_MoveAbsolute	✓		
MC_MoveRelative	✓		
MC_MoveVelocity	✓		
MC_MoveJog	✓		
MC_MoveSuperimposed	✓		
MC_HaltSuperimposed	✓		
MC_Stop	✓		
MC_SetAxisSTW	✓		
MC_SaveAbsoluteEncoderData	✓		
MC_WriteParameter	✓		
MC_SetSensor		✓	
MC_MeasuringInput	✓		
MC_MeasuringInputCyclic	✓		
MC_AbortMeasuringInput	✓		
MC_OutputCam	✓		
MC_CamTrack	✓		
MC_GearIn	✓		
MC_GearInVelocity		✓	
MC_GearInPos		✓	
MC_PhasingRelative		✓	
MC_PhasingAbsolute		✓	
MC_CamIn		✓	

¹ You can find this instruction under the main "Motion Control" Technology folder in STEP 7.

10.3 Motion Control instructions

MC instruction	Motion Control	Extended Motion Control	PTO Motion Control
MC_GearOut		✓	
MC_CamOut		✓	
MC_InterpolateCam		✓	
MC_GetCamLeadingValue		✓	
MC_GetCamFollowingValue		✓	
MC_GetCamFollowingValueCyclic ¹		✓	
MC_CopyCamData		✓	
MC_TorqueAdditive	✓		
MC_TorqueRange	✓		
MC_TorqueLimiting	✓		
MC_GroupInterrupt		✓	
MC_GroupContinue		✓	
MC_GroupStop		✓	
MC_MoveLinearAbsolute		✓	
MC_MoveLinearRelative		✓	
MC_MoveCircularAbsolute		✓	
MC_MoveCircularRelative		✓	
MC_MoveDirectAbsolute		✓	
MC_MoveDirectRelative		✓	
MC_DefineWorkspaceZone		✓	
MC_SetWorkspaceZoneActive		✓	
MC_SetWorkspaceZoneInactive		✓	
MC_DefineTool		✓	
MC_SetTool		✓	
MC_Power_PTO			✓
MC_Reset_PTO			✓
MC_MoveAbsolute_PTO			✓
MC_MoveRelative_PTO			✓
MC_MoveVelocity_PTO			✓
MC_MoveJog_PTO			✓
MC_Halt_PTO			✓
MC_Home_PTO			✓

¹ You can find this instruction under the main "Motion Control" Technology folder in STEP 7.

MC instruction	Motion Control	Extended Motion Control	PTO Motion Control
MC_ChangeDynamic_PTO			✓
MC_ReadParam_PTO			✓
MC_WriteParam_PTO			✓

¹ You can find this instruction under the main "Motion Control" Technology folder in STEP 7.

You can find help on programming each MC instruction in the TIA Portal Information System, as defined for the S7-1500/S7-1500T. These instructions are equivalent in S7-1200 G2. "_PTO" instructions, however, are unique to S7-1200 G2 and are defined as such in the TIA Portal Information System.

10.4 Motion Control Organization Blocks (OBs)

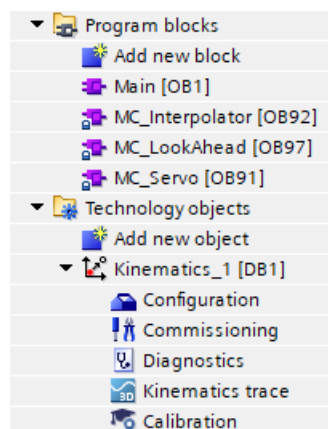
You can use an organization block (OB) to control how the CPU executes STEP 7 programs and handles interrupts and events. For Motion Control, this might mean executing closed-loop position control algorithms of TOs, monitoring and generating setpoints, or executing logic to create the desired movement of the axis.

Generated OBs

There are two types of OBs related to motion control. User OBs allow you to enter your motion control logic. Compiler-generated OBs are protected blocks and cannot be edited.

Supporting OBs

STEP 7 creates supporting organization blocks (OB) when you create a TO in your project.



G2-supported OBs

The S7-1200 G2 CPU provides support for the following Motion Control OBs:

- MC_PreServo (Page 119) - the CPU calls MC_PreServo immediately before MC_Servo, allowing you to make adjustments before the Servo logic executes.
- MC_Servo (Page 117) - performs calculations required to control the speed and position of axes. This block is protected.
- MC_PostServo (Page 119) - the CPU calls MC_PostServo immediately after MC_Servo executes, allowing you to modify outputs.
- MC_PreInterpolator - the CPU calls MC_PreInterpolator immediately before MC_Interpolator executes, allowing you to adjust inputs used by MC_Interpolator. These inputs will be IPO-synchronous.
- MC_Interpolator (Page 117) - evaluates Motion Control instructions, generates setpoints, and monitors inputs. This block is protected.
- MC_LookAhead (Page 120) - calculates motion processing for the Kinematics TO. This block is protected.

You can find help on programming each Motion Control OB in the TIA Portal Information System, as defined for the S7-1500/S7-1500T. These OBs are equivalent in S7-1200 G2.

10.5 Differences between S7-1200 G2 and S7-1500/S7-1500T

S7-1200 G2 Motion Control is similar In function to that of the S7-1500/1500T, with the following notable additions:

- Support for a subset of Extended Motion Control
- Support for a subset of Kinematics devices
 - Kinematics Cartesian Portal up to 3D with Orientation
 - SCARA up to 3D with Orientation
- Support for a subset of Cam TOs
- Support for Cam segments and VDI optimization

S7-1200 G2 Motion Control is similar In function to that of the S7-1500/1500T, with the following notable differences:

- No support for Kinematics Zones
- No support for User Defined Kinematics; however, Workspaces are supported
- No support for distributed motion control
- No support for TO_Cam_10k, TO_Cam_6kSeg, or TO_Cam_600Seg

10.5.1 Adapting Motion Control to S7-1200 G2

S7-1200 G2 motion control differs from that of the S7-1200. The S7-1200 G2 CPU uses Motion Control based upon the same technology used by the S7-1500/S7-1500T. In addition, however, the S7-1200 G2 uses a modified Basic Motion Control, which differs from the S7-1200 implementation. For these reasons, you cannot load an S7-1200 project with motion control into an S7-1200 G2 CPU.

There are differences between servo and PTO axes, such as the PLCOpen block layout and error codes. Refer to the PLCOpen standards for more information.

To learn about how Basic Motion Control operates in the S7-1200 G2 CPU, see the S7-1200 G2 Motion Control Function Manual

(<https://support.industry.siemens.com/cs/us/en/view/109995039>).

Migration paths

You must manually port your S7-1200 motion control projects into S7-1200 G2. Consider the following when performing this migration:

- The TOs are different
 - BMC objects are now contained within the folder "Motion PTO" and possess the suffix "_PTO".
 - Only PTO is supported. If you used PTO in your S7-1200 project, choose the relevant "_PTO" block. If you used Analog or PROFIdrive in your S7-1200 project, select the relevant block from the Standard Motion Control library.
 - TO_CommandTable is not supported.
 - Configuration interfaces in STEP 7 differ.
- The MC library is different
 - The "Motion Control" folder now contains both SMC and AMC blocks, while you can find the new BMC blocks in "Motion PTO".
 - You must drop and replace new blocks from the new library.
 - The behavior of most blocks is the same across libraries, though some names have changed.
 - Some MC instructions no longer exist.

You must manually port your S7-1500(T) motion control projects into S7-1200 G2. Consider the following when performing this migration:

- The TOs are different
 - Select the relevant blocks from the S7-1200 G2 Standard Motion Control library to replace those in your S7-1500(T) project using Analog or PROFIdrive.
 - Configuration interfaces in STEP 7 differ. While the functionality of both CPUs is identical, in some instances the S7-1200 G2 supports fewer configuration options.
- The MC library is different
 - You must drop and replace new blocks from the new library.
 - The behavior of most blocks is the same across libraries.
 - Some MC instructions are not available.
- Some tags in the PositioningAxis_PTO TO must be activated in the user program

10.6 Additional information

To active these tags, do the following:

1. Disable the PositioningAxis_PTO TO.
2. Download your new PositioningAxis_PTO configuration.
3. Execute MC_Reset_PTO with Restart = TRUE or transition the PLC from STOP to RUN.

NOTE

This is not a comprehensive list of differences.

NOTE

Compiling errors when copying Basic Motion Control blocks

Whenever you attempt to copy a Basic Motion Control block from an S7-1200 project to an S7-1200 G2 project in STEP 7 and download to your CPU, compiling errors occur. To avoid errors, you should instead first create a new TO_PositioningAxis_PTO in your S7-1200 G2 project before adding Basic Motion Control blocks.

10.6 Additional information

Siemens offers additional support for S7-1200 G2 Motion Control.

See also

You can learn more about Motion Control topics through the TIA Portal Information System.

You can also refer to the family of Motion Control V9.0 manuals available through Siemens Industry Online Support (<https://support.industry.siemens.com/cs/us/en/view/109974347>).

PID

11.1 PID functionality

STEP 7 provides the following PID instructions for the S7-1200 G2 CPU:

- The PID_Compact instruction is used to control technical processes with continuous or PWM input variables.
- The PID_3Step instruction is used to control motor-actuated devices, such as valves that require discrete signals for open- and close actuation or analog signal for specification of the target position.
- The PID_Temp instruction provides a universal PID controller that allows handling of the specific requirements of temperature control.

NOTE

Changes that you make to the PID configuration and download in RUN do not take effect until the CPU transitions from STOP to RUN mode. Changes that you make in the "PID parameters" dialog might not take effect immediately.

All three PID instructions (PID_Compact, PID_3Step, and PID_Temp) can calculate the proportional, integral, and derivative parameters for your controlled system during pretuning. You can also use fine tuning to tune the parameters further. You do not need to manually determine the parameters.

NOTE

Execute the PID instruction at constant intervals of the sampling time, preferably in a cyclic OB. Do not execute the PID instruction in the main program cycle OB, such as OB 1.

The sampling time of the PID algorithm represents the time between two calculations of the output value (control value). The sampling time of the PID algorithm is calculated during self-tuning and rounded to a multiple of the cycle time. All other functions of PID instruction are executed at every call.

PID algorithm

The output value for the PID controller consists of three components:

- P (proportional): When calculated with the "P" component, the output value is proportional to the difference between the setpoint and the process value (input value).
- I (integral): When calculated with the "I" component, the output value increases in proportion to the duration and value of the difference between the setpoint and the process value (input value) to correct the difference.
- D (derivative): When calculated with the "D" component, the output value increases as a function of the rate of change of the difference between the setpoint and the process value (input value). The process value is corrected to the setpoint as quickly as possible.

The PID controller uses the following formula to calculate the output value for the PID_Compact and PID_Temp instructions.

$$y = K_p \left[(b \cdot w - x) + \frac{1}{T_i \cdot s} (w - x) + \frac{T_d \cdot s}{a \cdot T_d \cdot s + 1} (c \cdot w - x) \right]$$

y	Output value	x	Process value
w	Setpoint value	s	Laplace operator
K _p	Proportional gain (P, I, D components)	a	Derivative delay coefficient (D component)
T _i	Integral action time (I component)	b	Proportional action weighting (P component)
T _d	Derivative action time (D component)	c	Derivative action weighting (D component)

The PID controller uses the following formula to calculate the output value for the PID_3Step instruction.

$$\Delta y = K_p \cdot s \cdot \left[(b \cdot w - x) + \frac{1}{T_i \cdot s} (w - x) + \frac{T_d \cdot s}{a \cdot T_d \cdot s + 1} (c \cdot w - x) \right]$$

y	Output value	x	Process value
w	Setpoint value	s	Laplace operator
K _p	Proportional gain (P, I, D components)	a	Derivative delay coefficient (D component)
T _i	Integral action time (I component)	b	Proportional action weighting (P component)
T _d	Derivative action time (D component)	c	Derivative action weighting (D component)

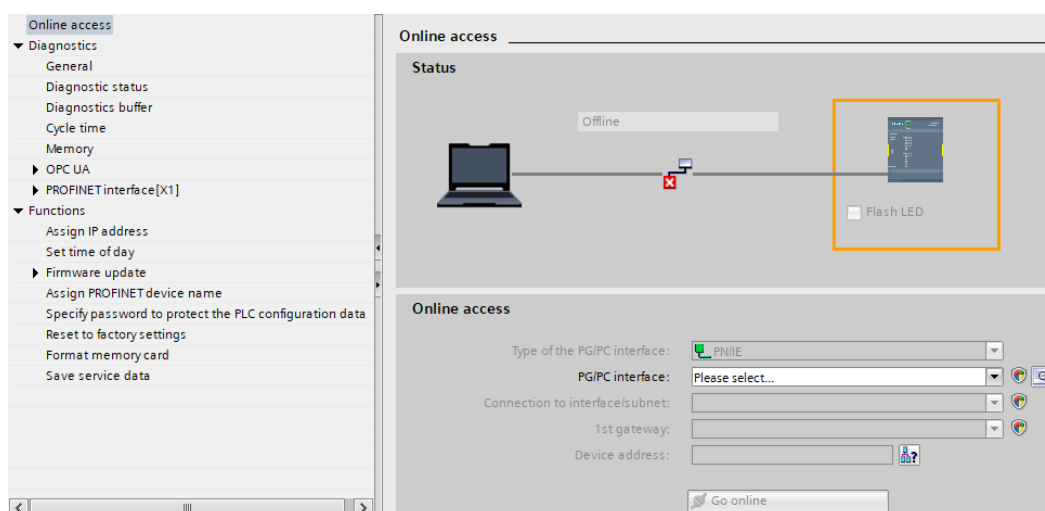
See also

For a comprehensive explanation of PID functions and instructions, see the "SIMATIC S7-1200, S7-1500 PID control" Function Manual (<https://support.industry.siemens.com/cs/us/en/view/108210036>), or find more information in the TIA Portal Information System.

Online and diagnostic tools

TIA Portal enables you to set diagnostic parameters and modify settings for the online behavior of your S7-1200 G2 CPU by using the tools listed below. You can update firmware, monitor cycle time and memory usage, and monitor or modify values in the CPU, in addition to other valuable functions.

To configure these parameters, select the CPU in the Project tree and select "Online & diagnostics" from the drop-down menu.



Tool	Description
Online access	
Online access	You can establish an online connection between the programming device and CPU for loading programs and project engineering data. For protected CPUs, you must enter either the access level CPU password or a user and user password. User roles and passwords are part of User Management and Access Control (UMAC) (Page 158) in the STEP 7 project.
Diagnostics	
General	Displays general information about the modules in your project.
Diagnostic status	Displays the status of diagnostic processes.
Diagnostics buffer (Page 133)	Use the diagnostics buffer to review the recent activity in the CPU. The diagnostics buffer is accessible from "Online & diagnostics" for an online CPU in the Project tree. It contains the following entries: - Diagnostic events - Changes in the CPU operating mode (transitions to STOP or RUN mode)
Cycle time	You can monitor the cycle time of an online CPU. After connecting to the online CPU, open the Online tools task card to view the relevant measurements.
Memory	You can monitor the memory usage (Page 129) of an online CPU. After connecting to the online CPU, open the Online tools task card to view the relevant measurements.

Tool	Description
PROFINET interface	You can use the PROFINET interface to view MAC addresses, IP Addresses, and Port settings.
OPC UA	You can configure the CPU as an OPC UA server for data access and view the status of the server, as well as diagnostic information about the sessions running on the server.
Functions	
Assign IP address	After accessing "Online & diagnostics" from the Project tree for an online CPU, you can display or change the IP address.
Set time	You can display or set the time and date parameters of the online CPU.
Firmware update	You can update the firmware of a connected CPU from the TIA Portal online and diagnostics tools using one of two methods: - Updating from the CPU in the project - Updating from the accessible devices in the project tree
Assign PROFINET device name	The devices on your PROFINET network must have an assigned name before you can connect with the CPU. Use the "Devices & networks" editor to assign names to your PROFINET devices if the devices have not already been assigned a name, or if the name of the device is to be changed.
Specify password to protect the PLC configuration data	The "Protection of confidential PLC configuration data" feature allows you to protect each CPU in your project individually. From the device configuration, you can enable this protection and set a password for the "protection of confidential PLC configuration data". Clients such as TIA Portal and the SIMATIC Automation Tool can only access the confidential data in the PLC through use of the password. You can also use the security wizard to enable this feature and set the password for the "Protection of confidential PLC configuration data".
Reset to factory settings	You can reset an S7-1200 G2 CPU to its original factory settings under the following conditions: - The CPU has an online connection. - The CPU is in STOP mode. If you reset the CPU to factory defaults, the CPU time will be reset to its default value.
Format memory card	You can format the memory card in a connected CPU from the TIA Portal online and diagnostic tools.
Save service data	In the event of servicing, the SIEMENS Customer Support requires information about the state of a module of your system for diagnostic purposes. If such a case occurs in your system, Customer Support can ask you to save the service data of the module and send the resulting file to them.
Online	
Backup and restore	You can create backups of your CPU configuration and software in the TIA Portal to be restored at a later point. This feature is available through the TIA Portal, the Web server, and the SIMATIC Automation Tool.

You can learn more about the above Tool properties by referring to the related topics in the TIA Portal Information System.

12.1 Status LEDs

The CPU and the I/O modules use LEDs to provide information about the operating state of the CPU and status of the devices.

Status LEDs on a CPU

The CPU provides the following status indicators:

- STOP/RUN
 - Solid yellow indicates STOP mode
 - Solid green indicates RUN mode
 - Flashing (alternating green and yellow) indicates that the CPU is in the STARTUP operating state
- ERROR
 - Flashing red indicates an error, such as an internal error in the CPU, an error with the memory card, or a configuration error (mismatched modules)
 - Flashing red for three seconds indicates a temporary error. An example is if the real-time clock (RTC) resets to the default time due to a power loss. Another example would be the failure of an NFC transaction.
 - Defective state:
 - STOP (ON), ERROR (Blinking), MAINT (Blinking)
- MAINT (Maintenance) is ON whenever maintenance is required, or if the NFC tag is defective while NFC is enabled in Device Configuration.

You can also use the LED instruction to determine the status of the LEDs.

Table 12-1 Status LEDs for a CPU

Description	RUN/STOP Green / Yellow	ERROR Red	MAINT Yellow
CPU power off	Off	Off	Off
CPU power up	Flashing (alternating yellow and green) ¹	Flashing ¹	Flashing ¹
STARTUP state	Flashing (alternating yellow and green)	-	Off
Firmware update in progress	Flashing (yellow)	-	-
Firmware update complete	-	-	Flashing
STOP state	On (yellow)	-	-
RUN state	On (green)	-	-
Missing program memory card (Page 142) (if External Load Memory used)	On (yellow)	Flashing	-

¹ When power is applied to the CPU, all three system-status indicators flash such that ERROR and MAINT are both ON when RUN/STOP is yellow and both OFF when RUN/STOP is green.

² Cyclically; three seconds Flashing, one second pause.

³ For each NFC transaction failure between CPU and NFC tag, the ERROR LED flashes three times.

12.1 Status LEDs

Description	RUN/STOP Green / Yellow	ERROR Red	MAINT Yellow
Memory card evaluation	Flashing (yellow)	-	-
Error	On (either yellow or green)	Flashing	-
Forced I/O	On (either yellow or green)	-	On
NFC defective, NFC enabled in configuration	On (either yellow or green)	-	On
NFC transaction failure	On (either yellow or green)	Flashing (3x) ³	-
Defective hardware (Page 336)	On (yellow)	On	Off
LED test or defective CPU firmware (Page 336)	Flashing (alternating yellow and green)	Flashing	Flashing
Unknown or incompatible version of CPU configuration (Page 336)	On (yellow)	Flashing	Flashing
Flash LED (Online access feature to identify CPU) ²	Flashing (alternating yellow and green)	Flashing	Flashing
Internal Load Memory was erased	Flashing (yellow)	Off	Flashing
Internal Load Memory is empty	Flashing (3 seconds) (yellow)	Off	Flashing (3 seconds)
Low battery powering the real-time clock (2.5 V or less remaining)	-	-	On

¹ When power is applied to the CPU, all three system-status indicators flash such that ERROR and MAINT are both ON when RUN/STOP is yellow and both OFF when RUN/STOP is green.

² Cyclically; three seconds Flashing, one second pause.

³ For each NFC transaction failure between CPU and NFC tag, the ERROR LED flashes three times.

Status LEDs for onboard I/O

Each CPU shall provide an I/O channel indicator for each onboard digital input and output, according to the table below:

Description	Digital I/O Channel (Green)
CPU power off	Off
Input or output point is Off	Off
Input or output point is On	On

Status LEDs for communication on the CPU

The CPU also provides two LEDs that indicate the status of the PROFINET communications. These LEDs are visible from the top of the CPU near the PROFINET connectors. Each PROFINET port has one LED which behaves according to the table below:

Description	PROFINET port (Green)
CPU power off	Off
Link down (no connection established)	Off
Link up (connection established)	On
Communication activity	Flashing

Status LEDs on a Signal Module (SM) and a Signal Board (SB)

Each digital or analog SM/SB provides a DIAG LED that indicates the status of the module or board:

- Green indicates that the module or board is operational
- Red indicates that the module or board is defective or non-operational

Each digital module or board provides an I/O Channel LED for each of the digital inputs and outputs.

- Green indicates the channel is ON
- OFF indicates the channel is OFF

Each analog module or board provides an I/O Channel LED for each of the analog inputs and outputs.

- Green indicates that the channel has been configured and is active
- Red indicates an error condition of the individual analog input or output

Each analog SB/SM provides an I/O Channel LED for each of the analog inputs and outputs, according to the following table:

Table 12-2 Status LEDs for an analog signal board (SB) or analog signal module (SM)

Description	DIAG (Green/Red)	Analog I/O Channel (Green/Red)
I/O bus power off, user power either on or off	Off	Off
I/O bus power on, user power off		
• Power fault diagnostic is enabled	Flashing (red)	Off
• Power fault diagnostic is disabled	On (green)	On (green)
STARTUP, but not yet logged into the CPU	Flashing (red)	Off

¹ Flashing the LED is only possible when the firmware is operational.

² The red DIAG LED acts like a summary fault indication which includes module errors and channel errors with channel diagnostics enabled.

12.1 Status LEDs

Description	DIAG (Green/Red)	Analog I/O Channel (Green/Red)
Logged in, but not yet configured	Flashing (green)	Off
Module configured with no errors	On (green)	On (green), all enabled channels
Error ^{1 2}		
• Module error	Flashing (red)	Flashing (red), all channels
• Channel error with channel diagnostic enabled	Flashing (red)	Flashing (red), affected channel
• Channel error with channel diagnostic disabled	On (green)	On (green), affected channel
Firmware update is running	Flashing (green)	Off

¹ Flashing the LED is only possible when the firmware is operational.

² The red DIAG LED acts like a summary fault indication which includes module errors and channel errors with channel diagnostics enabled.

Each digital SB/SM provides an I/O Channel LED for each of the digital inputs and outputs, according to the following table:

Table 12-3 Status LEDs for a digital signal board (SB) or digital signal module (SM)

Description	DIAG (Green/Red)	Digital I/O Channel (Green)
I/O bus power off, user power either on or off	Off	Off
I/O bus power on, user power off		
• Power fault diagnostic is enabled	Flashing (red)	Off
• Power fault diagnostic is disabled	On (green)	Off
STARTUP, but not yet logged into the CPU	Flashing (red)	Off
Logged in, but not yet configured	Flashing (green)	Off
Module configured with no errors		
• Input or output point is Off	On (green)	Off
• Input or output point is On	On (green)	On
Error	Flashing (red)	Off
Firmware update is running	Flashing (green)	Off

Serial communications indicators on a Communication Module (CM)/Communication Board (CB)

Each serial communications CM/CB provides a single DIAG indicator (green/red), plus a TxD transmit (yellow) and a RxD receive (yellow) indicator, according to the following table:

Description	DIAG Green / Red	TxD (yellow)	RxD (yellow)
I/O bus power off	Off	Off	Off
STARTUP, but not yet logged into CPU	Flashing (red)	-	-
Logged in, but not yet configured	Flashing (green)	-	-
Module configured with no errors - Transmit data in process - Receive data in process	On (green)	On -	- On
Error	Flashing (red)	-	-
Firmware update is running	Flashing (green)	Off	Off

Battery Board (BB) indicator

The battery board provides a single DIAG indicator (green/red), according to the following table:

Description	DIAG Green / Red
CPU power off	Off
STARTUP, but not yet logged into CPU	Flashing (red)
Logged in, but not yet configured	Flashing (green)
Configured with no errors	On (green)
Error: voltage detected to be below the allowed threshold	Flashing (red)

12.2 CPU error behavior

"Unknown or incompatible version of CPU configuration" error

The diagnostics buffer can report an "Unknown or incompatible version of CPU configuration" error, which can occur in one of the following ways:

- Attempting to load an invalid project.
- Attempting to download a project with different protection of confidential PLC configuration data (Page 329) between the CPU and the project

If you reached this state by using an invalid version transfer card (Page 146), follow these steps to recover:

1. Remove the transfer card.
2. Perform a STOP to RUN transition.
3. Reset the memory (MRES) or cycle power.

If you reach this state by using an invalid project on a program card (Page 148), reset the CPU to factory settings (Page 329) using the "Format memory card" option .

If you reach this state from a mismatch between the CPU and the project for the protection of confidential PLC configuration data, use the Online & Diagnostics tools (Page 329) to set the online CPU's password for protection of confidential PLC configuration data to the password in the project, or delete it from the online CPU.

After you recover the CPU from the error condition, you can download a valid program.

S7-1200 G2 behavior following a fatal error

If the CPU firmware detects a fatal error, it attempts a defect-mode restart, and if successful, signals the defective mode by continually flashing the STOP/RUN, ERROR and MAINT LEDs.

If the CPU successfully completes the defect-mode restart, the CPU performs these actions:

- Sets the CPU and signal board outputs to the configured value
- Sets the outputs of local rack signal modules and distributed I/O to the selection for "Reaction to CPU STOP" in the device configuration of the digital outputs of the module

If the defect-mode restart fails, (for example, due to a hardware fault), the STOP and ERROR LEDs are ON and the MAINT LED is OFF.



WARNING

Operation in defect state cannot be guaranteed

Control devices can fail in an unsafe condition, resulting in unexpected operation of controlled equipment.

Use an emergency stop function, electromechanical overrides or other redundant safeguards that are independent of the PLC.

Such unexpected operations can result in death or serious injury to personnel, and/or damage to equipment.

12.3 Analog module diagnostics

Analog modules have multiple diagnostics depending on the module and channel type. You can separately enable or disable these diagnostics for each module and channel by using the TIA Portal under the project's device configuration/general properties of the module.

Power supply errors are reported as follows:

Power supply error	Error reported
Analog module with a power supply diagnostic error reports:	Overflow: 32767 for all input channels
	Missing power supply diagnostic, if enabled for output modules

You can enable these diagnostics separately by channel and type for each channel. See the table below:

Channel type	Error reported
Voltage input	Overflow: 32767
	Underflow: -32768
Current input (0 to 20 mA)	Overflow: 32767
	Underflow: -32768
Current input (4 to 20 mA) (for < 1.185 mA input)	Broken wire: 32767
	Overflow: 32767
Voltage output (for > 0.5 V output)	Short circuit diagnostic, if enabled
Current output (for > 1.0 mA output)	Open circuit diagnostic, if enabled
RTD input	Broken wire: 32767
	Overflow: 32767
	Underflow: -32768
Resistor input	Broken wire: 32767
	Overflow: 32767
Thermocouple input	Broken wire: 32767
	Overflow: 32767
	Underflow: -32768

An analog input module with a diagnostic error on any channel reports 32767 or -32768 on that channel even if the diagnostics is not enabled. Analog input channels report 32767 when deactivated.

12.4 Comparing offline and online CPUs

You can compare the code blocks in an online CPU with the code blocks in your project. If the code blocks of your project do not match the code blocks of the online CPU, the "Compare" editor allows you to synchronize your project with the online CPU by downloading the code blocks of your project to the CPU, or by deleting blocks from the project that do not exist in the online CPU.

NOTE

Read access required on protected CPU for the Offline/Online compare operations

For TIA Portal, the "HMI access" security level is insufficient to perform the Offline/Online compare operations. You must have "Read access" or "Full access", to do Offline/Online compare operations.

See also Protection & Security in CPU properties (Page 166).

You can learn more about comparing offline/online CPUs, as well as their related topologies in your network, by referring to the TIA Portal Information System.

12.5 Monitoring and modifying values in the CPU

12.5.1 Overview of the online monitoring and modification tools

TIA Portal provides online tools for monitoring the CPU:

- You can display or monitor the current values of the tags. The monitoring function does not change the program sequence. It presents you with information about the program sequence and the data of the program in the CPU.
- You can also use other functions to control the sequence and the data of the user program:
 - You can modify the value for the tags in the online CPU to see how the user program responds.
 - You can force a peripheral output (such as Q0.1:P or "Start":P) to a specific value.

NOTE

Always exercise caution when using control functions. These functions can influence the execution of the user/system program.

Table 12-4 Online capabilities of the TIA Portal editors

Editor	Monitor	Modify	Force
Watch table	Yes	Yes	No
Force table	Yes	No	Yes
Program editor	Yes	Yes	No
Tag table	Yes	No	No
DB editor	Yes	Yes	No

You can learn more about online tools for monitoring the CPU by referring to the related topics in the TIA Portal Information System.

12.5.2 Watch tables for monitoring the user program

A watch table allows you to perform monitoring and control functions on data points as the CPU executes your program. These data points can be process image (I or Q), M, DB or physical inputs (I_:P), depending on the monitor or control function. You cannot accurately monitor the physical outputs (Q_:P) because the monitor function can only display the last value written from Q memory and does not read the actual value from the physical outputs.

The monitoring function does not change the program sequence. It presents you with information about the program sequence and the data of the program in the CPU.

Control functions enable the user to control the sequence and the data of the program. You must exercise caution when using control functions. These functions can influence the execution of the user/system program. The two control functions are Modify and Force.

With the watch table, you can perform the following online functions:

- Monitoring the status of the tags
- Modifying values for the individual tags

You can learn more about using a watch table for monitoring and modifying values in the CPU by referring to the related topics in the TIA Portal Information System.

12.5.3 Using the force table

A force table provides a "force" function that overwrites the value for an input or output point to a specified value for the peripheral input or peripheral output address. The CPU applies this forced value to the input process image prior to the execution of the user program and to the output process image before the outputs are written to the modules.

You can learn more about forcing values in the CPU with the Force function by referring to the related topics in the TIA Portal Information System.

12.6 Downloading in RUN mode

12.6.1 Overview

The CPU supports "Download in RUN mode". This capability allows you to download program changes while the program is running.



WARNING

Risks when downloading in RUN mode

When you download changes to the CPU in RUN mode, the changes immediately affect process operation. Changing the program in RUN mode can result in unexpected system operation.

Only authorized personnel who understand the effects of RUN mode changes on system operation should perform a download in RUN mode.

Unexpected system operation can cause death or serious injury to personnel, and/or damage to equipment.

The "Download in RUN mode" feature allows you to make changes to a program and download them to your CPU without switching to STOP mode:

- You can make minor changes to your current process without having to shut down (for example, change a parameter value).
- You can debug a program more quickly with this feature (for example, invert the logic for a normally open or normally closed switch).

You can make the following program block and tag changes and download them in RUN mode:

- Create, overwrite, and delete Functions (FC), Function Blocks (FB), and Tag tables.
- Create, delete, and overwrite Data Blocks (DB) and instance data blocks for Function Blocks (FB). You can add to DB structures and download them in RUN mode. The CPU can maintain the values of existing block tags and initialize the new data block tags to their initial values, or the CPU can set all data block tags to initial values, depending on your configuration settings.
- Create, overwrite, modify, and delete Organization Blocks (OB).

You can download a maximum number of 20 blocks in RUN mode at one time. If you need to download more than 20 blocks, you must place the CPU in STOP mode.

If you download changes to a running process, you must think through the possible safety consequences to machines and machine operators before you download.

NOTE

If the CPU is in RUN mode and program changes have been made, TIA Portal always tries to download in RUN first. If you do not want this to happen, you must put the CPU into STOP.

If the changes made are not supported in "Download in RUN", TIA Portal prompts you that the CPU must go to STOP.

12.6.2 Prerequisites for "Download in RUN mode"

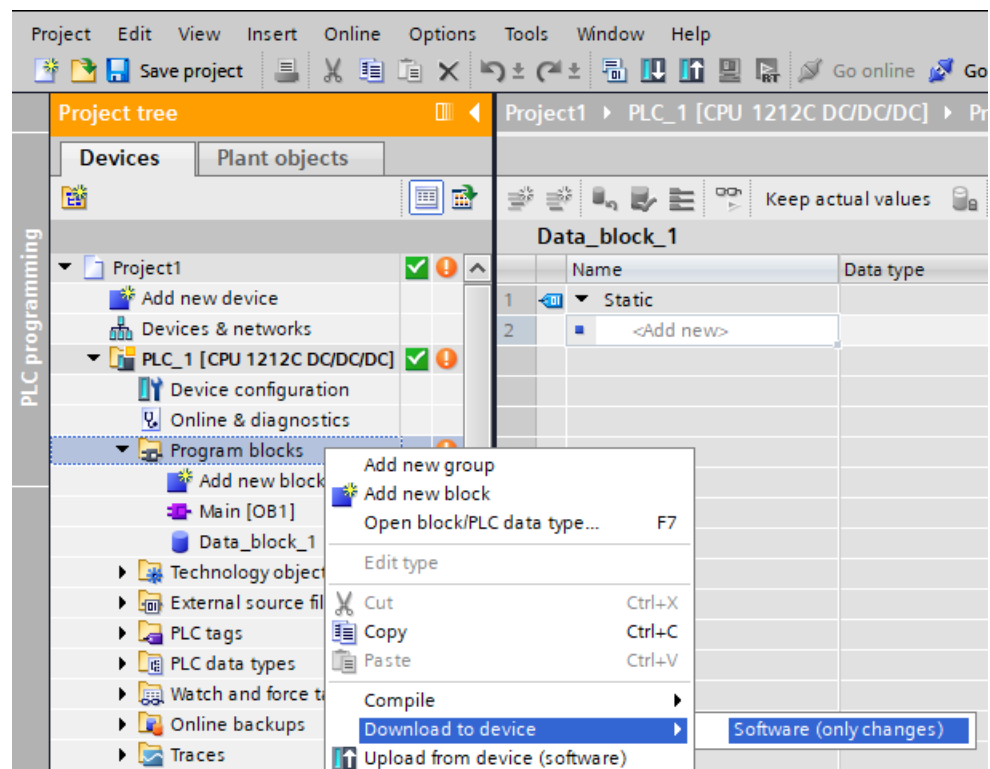
To be able to download your program changes to a CPU that is in RUN mode, you must meet these prerequisites:

- Your program blocks must compile successfully.
- You must have successfully established communication between the CPU and the programming device.

12.6.3 Changing your program in RUN mode

To change the program in RUN mode, you must first ensure that the CPU and program meet the prerequisites [\(Page 341\)](#), and then follow these steps:

1. To download your program in RUN mode, select one of the following methods:
 - Select the "Download to device" command from the "Online" menu.
 - Click the "Download to device" button in the toolbar.
 - In the "Project tree", right-click "Program blocks" and select the "Download to device > Software (only changes)" command.



If the program compiles successfully, TIA Portal starts to download the program to the CPU. You might be prompted for choices about synchronization.

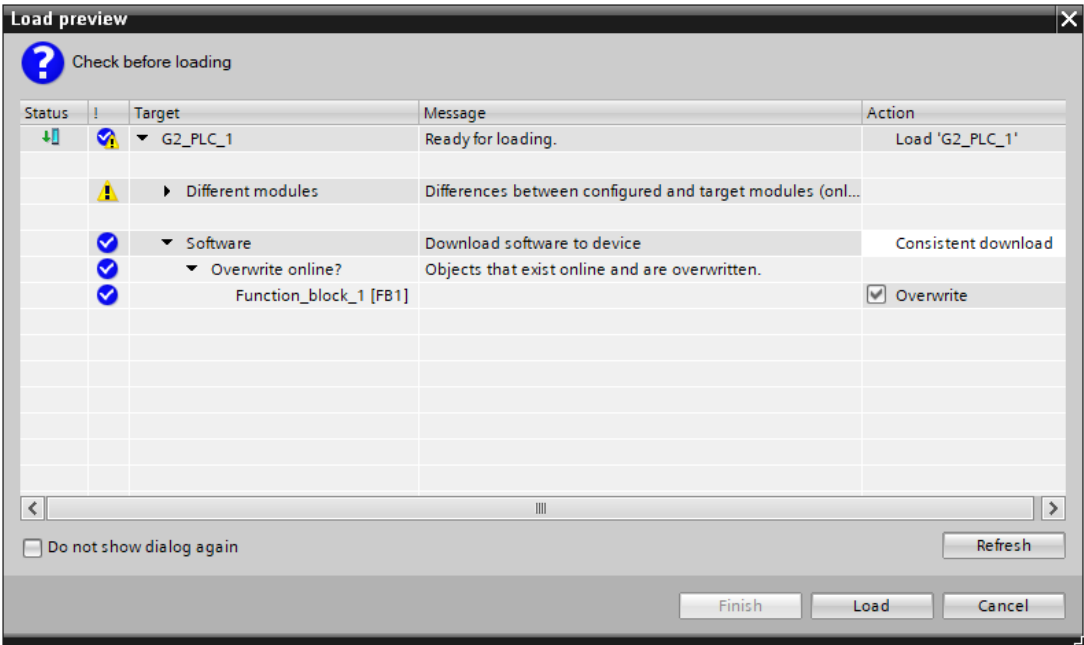
2. When TIA Portal prompts you to load your program or cancel the operation, click "Load" to download the program to the CPU.

12.6.4 Downloading selected blocks

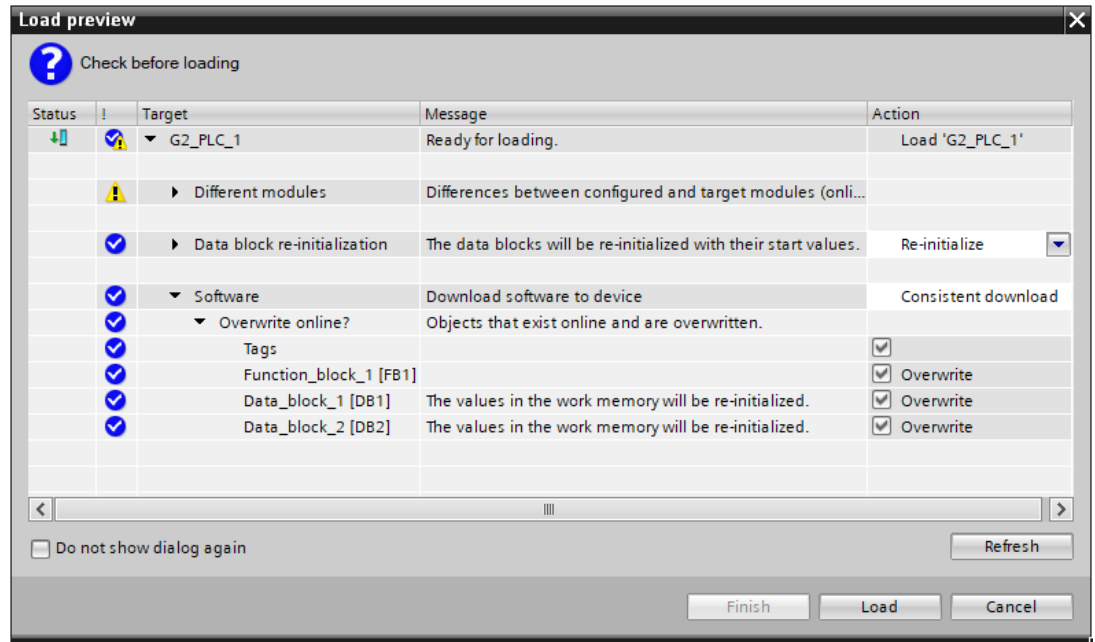
From the Program blocks folder, you can select a single block or a selection of blocks for downloading.

If you select a single block for downloading, then the only option in the "Action" column is "Consistent download".

You can expand the category line to be sure what blocks are to be loaded. In this example, a small change was made to the offline block, and no other blocks need to be loaded.



In this example, more than one block is needed for downloading.



NOTE

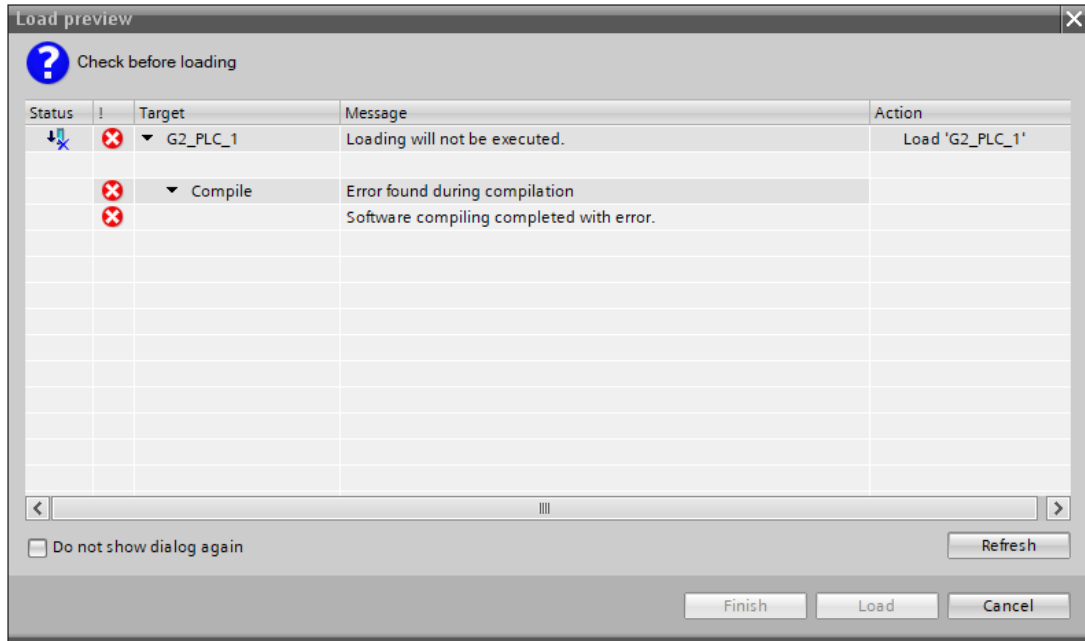
You can download a maximum number of 20 blocks in RUN mode at one time. If you need to download more than 20 blocks, you must place the CPU in STOP mode.

If you attempt to download in RUN, but the system detects that this is not possible, you must put the CPU in STOP mode.

Click the "Load" button, and the "Load results" dialog appears. Click the "Finish" button to complete the download.

12.6.5 Downloading a single selected block with a compile error in another block

If you attempt a consistent download with a compile error in another block, then the dialog indicates an error, and the load button is disabled.



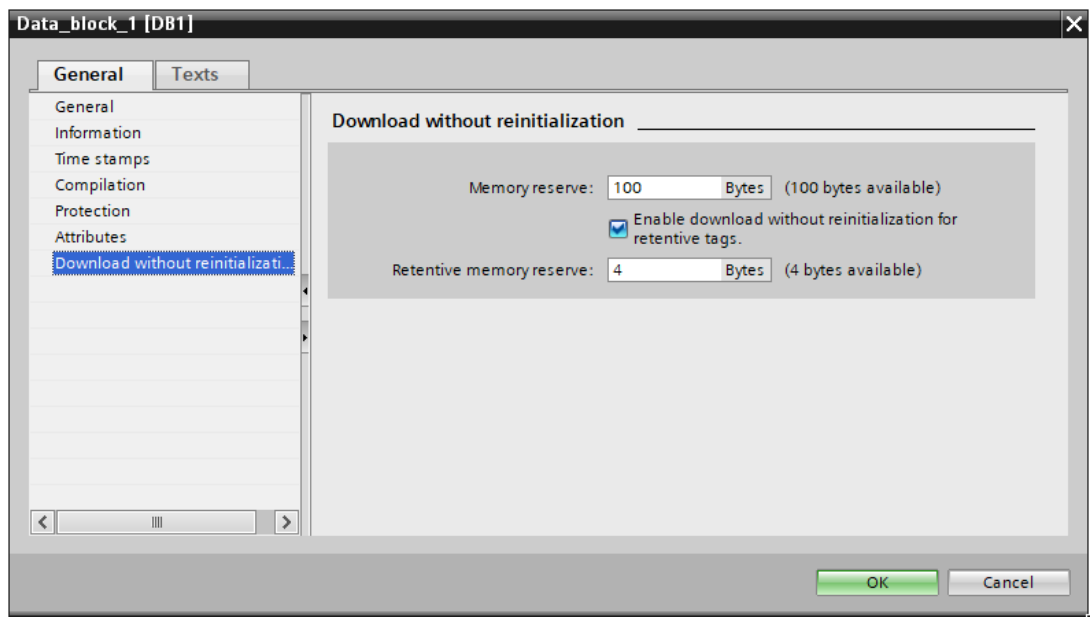
You must correct the compile error in the other block. Then, the "Load" button becomes active.

12.6.6 Modifying and downloading existing tags in RUN mode

The Download in Run feature allows you to add and modify tags in data blocks and function blocks and then download the changed block to the CPU in RUN mode.

Download without reinitialization

Each DB and FB has an amount of reserved memory, which you can use for adding tags to the block that you can subsequently download in RUN mode. By default, the initial size of the memory reserve is 100 bytes. You can add additional tags to your data up to the size of the memory reserve and download the extended block to the CPU in RUN mode. You can also increase the memory reserve if you need more memory for additional tags in your block. If you add more tags than the amount of memory you have allocated, you cannot download the extended block to the CPU in RUN mode.



The "Download without reinitialization" feature allows you to extend a data block by adding more data block tags and download the extended data block in RUN mode. In this way, you can add tags to a data block and download it without reinitializing your program. The CPU retains the values of the existing data block tags and initializes the newly-added tags to their start values.

To enable this function for an online project with a CPU in RUN mode, follow these steps:

1. From the Program blocks folder in the TIA Portal project tree, right-click the block and select "Properties".
2. Click "Download without reinitialization" and select the "Enable download without reinitialization for retentive tags" checkbox in the block editor to enable the function.
3. Click "OK" on the prompt to confirm your choice.
4. Add tags to the block interface and download the block in RUN mode. You can add and download as many new tags as your memory reserve allows.

If you have added more bytes to your block than you have configured for the memory reserve, TIA Portal displays an error when you attempt to download the block in RUN mode. You must edit the block properties to increase the amount. You cannot delete existing entries

or modify the "Memory reserve" of the block while the "Download without reinitialization" function is enabled. To disable the "Download without reinitialization" function, follow these steps:

1. From the Program blocks folder in the TIA Portal project tree, right-click the block and select "Properties".
2. Click "Download without reinitialization" and de-select the "Enable download without reinitialization for retentive tags" checkbox in the block editor to disable the function.
3. Click "OK" on the prompt to confirm your choice.
4. Download the block. On the download dialog, you must select "reinitialize" in order to download the extended block.

The download then reinitializes all existing and new block tags to their start values.

Downloading retentive block tags

Downloading retentive block tags in RUN mode requires the allocation of a retentive memory reserve. To configure this retentive memory reserve, follow these steps:

1. From the Program blocks folder in the TIA Portal project tree, right-click the block and select "Properties" from the context menu.
2. Select the "Download without reinitialization" property.
3. Select the check box for "Enable download without reinitialization for retentive tags".
4. Configure the number of bytes available for the retentive memory reserve.
5. Click "OK" to save your changes.
6. Add retentive data block tags to the data block and download the data block in RUN mode.

To add and download as many new retentive data block tags as your retentive memory reserve allows, click "Activate memory reserve" on the toolbar. For more information, refer to "Basic information on loading block extensions without reinitialization" in the TIA Portal Information System.

If you have added more retentive bytes to your data block than you have configured for the retentive memory reserve, TIA Portal displays an error when you attempt to download the block in RUN mode. You can only add retentive block tags up to the retentive memory reserve in order to be able to download them in RUN mode.

When you download the extended retentive block tags, the tags contain their current values.

Configuring amount of reserved memory for new blocks

The default memory reserve size for new data blocks is 100 bytes. When you create a new block, it has 100 bytes available in reserve. If you want the memory reserve size to be different for new blocks, you can change the setting in the PLC programming settings:

1. From TIA Portal, select the **Options > Settings** menu command.
2. From the Settings dialog, expand "PLC programming" and select "General".
3. In the "Download without reinitialization" section, enter the number of bytes for the memory reserve.

When you create new blocks, TIA Portal uses the memory reserve configuration that you entered for the new blocks.

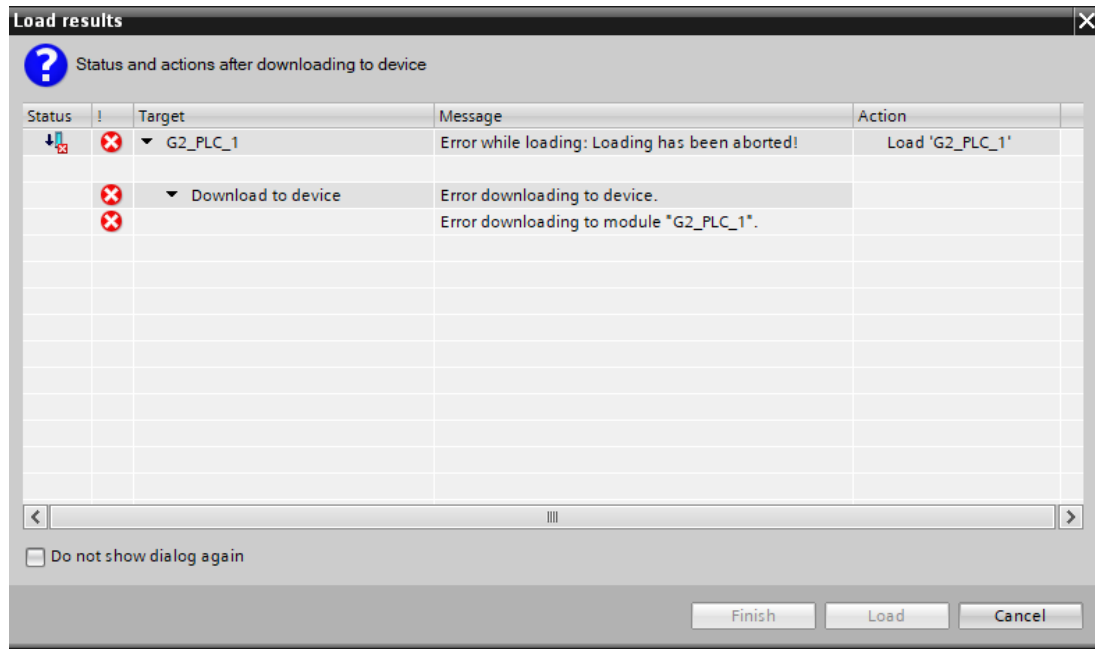
Restrictions

The following restrictions apply to editing and downloading blocks in RUN mode:

- Extending the block interface by adding new tags and downloading in RUN mode is only available for optimized blocks.
- You cannot change the structure of a block and download the changed block in RUN mode without reinitializing. Adding new members to a Struct tag, changing tag names, array sizes, data types, or retentive status all require that you reinitialize the block if you download it in RUN mode. The only modifications to existing block tags that you can perform and still download the block in RUN mode without reinitialization are changes to start values (data blocks), default values (function blocks) or comments.
- You cannot download more new block tags in RUN mode than the memory reserve can accommodate.
- You cannot download more new retentive block tags in RUN mode than the retentive memory reserve can accommodate.

12.6.7 System reaction if the download process fails

During the initial Download in RUN operation, if a network connection failure occurs, STEP 7 displays the following "Load results" dialog:



12.6.8 Considerations when downloading in RUN mode

Before downloading the program in RUN mode, consider the effect of a RUN-mode modification on the operation of the CPU for the following situations:

- If you deleted the control logic for an output, the CPU maintains the last state of the output until the next power cycle or transition to STOP mode.
- If you deleted a high-speed counter or pulse output functions which were running, the high-speed counter or pulse output continues to run until the next power cycle or transition to STOP mode.
- Any logic that is conditional on the state of the first scan bit will not be executed until the next power cycle or transition from STOP to RUN mode. The first scan bit is set only by the transition to RUN mode and is not affected by a download in RUN mode.
- The current values of data blocks (DBs) and/or tags can be overwritten.

Requirements

Before you can download your program in RUN mode, the program must compile with no errors, and the communication between TIA Portal and the CPU must be error-free.

You can make the following changes in program blocks and tags and download them in RUN mode:

- Create, overwrite, and delete Functions (FCs), Function Blocks (FBs), and Tag tables.
- Create and delete Data Blocks (DBs); however, DB structure changes cannot be overwritten. Initial DB values can be overwritten. You cannot download a Web server DB (control or fragment) in RUN mode.
- Create, overwrite, and delete Organization Blocks (OBs).

You can download a maximum number of 20 blocks in RUN mode at one time. If you need to download more than 20 blocks, you must place the CPU in STOP mode.

Once you initiate a download, you cannot perform other tasks in TIA Portal until the download completes.

Instructions that might fail due to "Download in RUN mode"

The following instructions might experience a temporary error when download in RUN mode changes are being activated in the CPU. The error occurs when the instruction is initiated while the CPU is preparing to activate the downloaded changes. During this time, the CPU suspends initiation of user-program access to the Load Memory, while it completes in-progress user program access to Load Memory. This is done so that downloaded changes can be activated consistently.

Instruction	Response while Activation is Pending
DataLogCreate	STATUS = W#16#80C0, ERROR = TRUE
DataLogOpen	STATUS = W#16#80C0, ERROR = TRUE
DataLogWrite	STATUS = W#16#80C0, ERROR = TRUE
DataLogClose	STATUS = W#16#80C0, ERROR = TRUE
DataLogNewFile	STATUS = W#16#80C0, ERROR = TRUE
DataLogClear	STATUS = W#16#80C0, ERROR = TRUE
DataLogDelete	STATUS = W#16#80C0, ERROR = TRUE
READ_DBL	RET_VAL = W#16#82C0
WRIT_DBL	RET_VAL = W#16#82C0
CREATE_DB	RET_VAL = W#16#80C0
DELETE_DB	RET_VAL = W#16#80C0
RTM	RET_VAL = W#16#80C0

In all cases the RLO output from the instruction will be false when the error occurs. The error is temporary. If it occurs, the instruction should be retried later.

If one of the above instructions fails to execute because a download in RUN mode was in process, retry the failed instruction in a subsequent execution of that OB. If you retry the instruction in the same OB execution, it will fail.

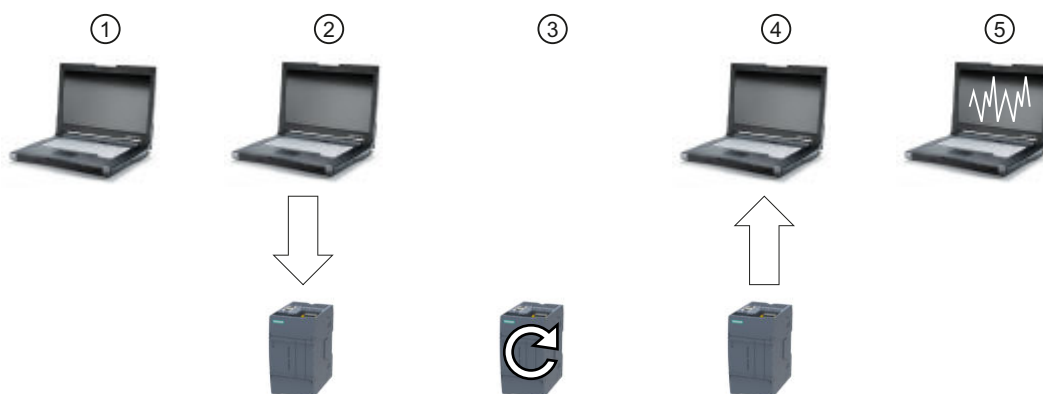
12.7 Tracing and recording CPU data on trigger conditions

TIA Portal provides trace and logic analyzer functions with which you can configure variables for the PLC to trace and record. You can then upload the recorded trace measurement data to your programming device and use TIA Portal tools to analyze, manage, and graph your data. You use the Traces folder in the TIA Portal project tree to create and manage traces.

NOTE

The trace measurement data is available only within the TIA Portal project and is not available for processing by other tools.

The following figure shows the various steps of the trace feature:



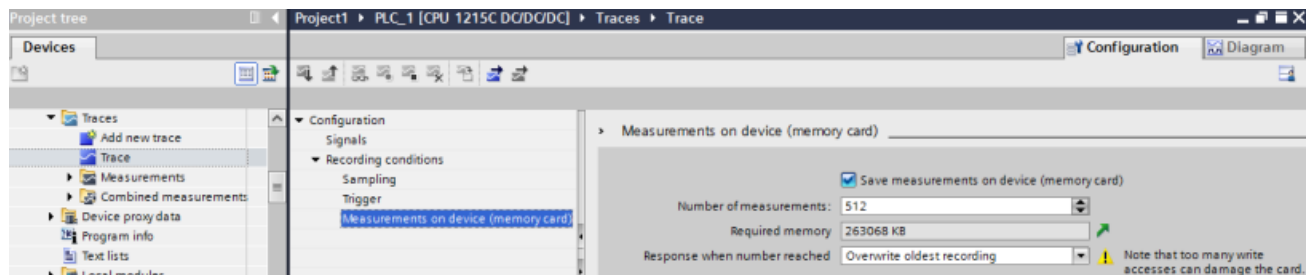
- ① Configure the trace in the trace editor of TIA Portal. You can configure the following options:
 - Data values to record
 - Recording duration
 - Recording frequency
 - Trigger condition
- ② Transfer the trace configuration from TIA Portal to the PLC.
- ③ The PLC executes the program, and when the trigger condition occurs, begins recording the trace data.
- ④ Transfer the recorded values from the PLC to TIA Portal.
- ⑤ Use the tools in TIA Portal to analyze, graphically display, and save the data.

The S7-1200 G2 supports four trace jobs with a maximum of 16 variables captured per trigger event. Each trace job provides 512 Kbytes of RAM for the recording of trace values and associated overhead, for example variable addresses and time stamps.

Saving trace measurements to the memory card

The S7-1200 G2 CPU can only save trace measurements to the SIMATIC memory card. If you do not have a memory card in your CPU, the CPU will log a diagnostics buffer entry if the program attempts to save trace measurements. The CPU limits the space allocated to trace measurements such that 1 MB of external load memory must always be available. If a trace measurement would require more memory than the maximum allowance, the CPU will not save the measurement and will log a diagnostics buffer entry.

In addition, if you select "Overwrite oldest recording" in TIA Portal, the continual writing can reduce the lifetime of load memory. When you select "Overwrite oldest recording", the CPU replaces the oldest measurement with the newest measurement after it has stored the configured number of trace measurements, and continues tracing and saving measurements. Overwriting the oldest measurements is useful in capturing intermittent problems.



The CPU supports a maximum of 1000 trace measurement results. During the time that the CPU is saving the trace measurements to external load memory, the CPU does not check the trigger condition for the trace job. Once the CPU finishes saving the trace measurements, the CPU resumes checking for trigger conditions.

Access to examples

See the TIA Portal Information System for details about how to program a trace, how to download the configuration, upload the trace data, and display the data in the logic analyzer. You can find detailed examples there in the "Using the trace and logic analyzer function" (https://docs.tia.siemens.cloud/access?ft:originId=../29275874699/29275874699_enUS.htm&ft:clusterId=../29275874699/29275874699.htm)" chapter.

In addition, the online manual "Industry Automation SINAMICS/SIMATIC Using the trace and logic analyzer function" (<https://support.industry.siemens.com/cs/us/en/view/64897128>) is an excellent reference.

12.8 Determining the type of error from an analog module

As described in the topic Analog module diagnostics (Page 337), an analog module returns an analog input value of 32767 (16#7FFF) for both a wire break condition and an overflow condition. These conditions apply to the channel only and not to the module. If you want to determine which of these two conditions occurred, you can include logic in your STEP 7 program to make the determination. The method to determine the condition type consists of these tasks:

- Create a Diagnostic error interrupt OB to be called whenever there is an incoming or outgoing diagnostic event.
- Include a call to the RALRM instruction.
- Set up an array of bytes for the AINFO parameter, which includes the information about the condition type.
- Evaluate bytes 32 and 33 of the AINFO structure of the RALRM_DB when the CPU triggers the Diagnostic Interrupt OB..

Creating a Diagnostic error interrupt OB

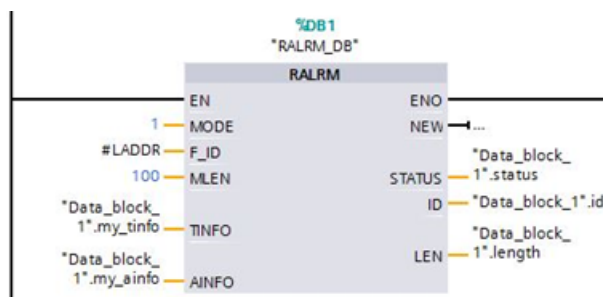
To be able to determine when a wire break condition occurs, create a Diagnostic error interrupt OB. The CPU calls this OB whenever an incoming or outgoing diagnostic event occurs.

When the CPU calls the Diagnostic error interrupt OB, the input parameter LADDR will contain the hardware identifier for the module with the error. You can find the hardware identifier for the SM 1231 module in the STEP 7 device configuration for the SM 1231 module.

Calling the RALRM instruction

To program the RALRM instruction call, follow these steps:

1. Add a call to RALRM in your STEP 7 program.
2. Set the F_ID input parameter to the hardware identifier in the LADDR parameter of the Diagnostic error interrupt OB.
3. Use an array of bytes for the TINFO and AINFO input parameters. Use an array size of 34 bytes or greater.



Interpreting AINFO after a diagnostic interrupt has occurred

The AINFO byte array will contain the information about the module diagnostics after the Diagnostic error interrupt OB executes.

Bytes 0 - 25 are header information. The bytes pertaining to the module diagnostic are as follows:

Byte	Description
26 and 27	Word value 16#8000 - indicates the diagnostic is a PROFINET style diagnostic
28 and 29	Word containing channel number responsible for this diagnostic
30	Bit pattern aaabb000 that indicates the type of channel (aaa) and type of error (bb)
	aaa
	bb
	000: reserved
	001: input channel
	010: output channel
	011: input/output channel
	00: reserved
	01: incoming error
	10: outgoing error
	11: outgoing error, other errors present
31	Indication of data format 0: Free data format 1: Bit 2: Two bits 3: Four bits 4: Byte 5: Word (two bytes) 6: Double word (four bytes) 7: Two double words (eight bytes)
32 and 33	Word that defines the type of error: 16#0000: reserved 16#0001: short circuit 16#0002: undervoltage 16#0003: overvoltage 16#0004: overload 16#0005: over temperature 16#0006: wire break 16#0007: high limit exceeded 16#0008: low limit exceeded 16#0009: error

For example, consider bytes 26 - 33 of this AINFO structure:

29	my_ainfo[26]	Byte	16#0	16#80
30	my_ainfo[27]	Byte	16#0	16#00
31	my_ainfo[28]	Byte	16#0	16#00
32	my_ainfo[29]	Byte	16#0	16#00
33	my_ainfo[30]	Byte	16#0	16#28
34	my_ainfo[31]	Byte	16#0	16#05
35	my_ainfo[32]	Byte	16#0	16#00
36	my_ainfo[33]	Byte	16#0	16#07

- The Word at bytes 26 and 27 is 16#8000, which indicates that this is a PROFINET style diagnostic.
- The Word at bytes 28 and 29 indicates this is a diagnostic for channel 0 or the module.
- Byte 30 is 16#28, which when interpreted as the bit pattern aaa bb 00 is 001 01 000. This value indicates that this diagnostic is for an input channel and is an incoming error.
- Byte 31 is 5, which indicates a Word value
- The word value at bytes 32 and 33 is 16#0007, which indicates high limit exceeded.

By capturing the AINFO information from a Diagnostic error interrupt event, you can thus determine the nature of the diagnostic event.

12.9 Backup and restore options

You can create a backup of your CPU. You can then restore this backup file to the CPU or to another CPU. You can find the backups in the project tree under the CPU in the "Online backups" folder.

Scope of the backup

The backup file contains the following:

- Contents of the memory card, if present
- Retentive memory areas (for example, data blocks, counters, and bit memory)
- Other retentive memory contents, such as IP address parameters

The backup is performed with the current values of the CPU. Entries in the diagnostics buffer are not included in the backup, and neither is the current time.

The backup does not contain the password to protect confidential PLC configuration data.

Backup and restore operations

STEP 7 and the S7-1200 G2 CPU offer the following options for backing up and restoring the hardware configuration and software:

- Snapshot of the actual values
- Upload from device (software)
- Upload device as new station (hardware and software)
- Backup from online device

To learn more about options for backing up and restoring your CPU, refer to the following:

- The topic "Creating a backup of an S7 CPU" (https://docs.tia.siemens.cloud/access?ft:originId=ProgOnlineBackupenUS_20.00.00.00_release&ft:clusterIdProgOnlineBackup) in the TIA Portal Information System
- The S7-1500/ET 200, SIMATIC Drive Controller Web server (<https://support.industry.siemens.com/cs/ww/en/view/109977246>) function manual
- The SIMATIC Automation Tool user guide (<https://support.industry.siemens.com/cs/us/en/view/109986787>)

Technical specifications

A.1 General technical specifications

Standards compliance

The S7-1200 G2 automation system design conforms with the following standards and test specifications. The test criteria for the S7-1200 G2 automation system are based on these standards and test specifications.

NOTE

Some S7-1200 G2 devices are not certified to all the following standards, and certification status can change without notice. Most certification approval markings are listed on the device or packaging. You are responsible for determining whether the devices in your system meet the required certifications for your application. For additional information on the certifications of a specific device, consult with a local Siemens representative or visit the Siemens Industry Online Support Web site (<https://sieportal.siemens.com/en-ww/support>). Device certificates can be downloaded from the Siemens Industry Online Support Web site.

CE approval



The S7-1200 G2 automation system satisfies requirements and safety related objectives according to the EC directives listed below, and conforms to the harmonized European standards (EN) for the programmable controllers listed in the Official Journals of the European Community.

- 2014/30/EU "Electromagnetic Compatibility" (EMC Directive)
- 2014/53/EU "Radio Equipment" (RED Directive)
- 2014/34/EU "Equipment and protective systems intended for use in potentially explosive atmospheres" (ATEX Directive)
- 2011/65/EU "Restriction of the use of certain hazardous substances in electrical and electronic equipment" (RoHS Directive)
- 2006/42/EC "Machinery Directive" for S7-1200 G2 F-CPU, F-SM, and F-SB modules

EU declarations of conformity for the respective authorities are available from:

Siemens AG
Digital Industries
Factory Automation
P.O. Box 1963
D-92209 Amberg

The EU declarations of conformity are also available for download from the Siemens Industry Online Support Web site (<https://sieportal.siemens.com/en-ww/support>), under the keyword "Declaration of Conformity".

Radio Equipment Directive (RED) compliance

The S7-1200 G2 automation system complies with the Radio Equipment Directive (RED) 2014/53/EU. The RED defines NFC tags as radio equipment. The frequency 13.56 MHz is regulated under ETSI EN 300 330 v2.1.1.

UK Conformity Assessed marking



The S7-1200 G2 automation system complies with the designated British standards (BS) for programmable controllers published in the official consolidated list of the British Government. The S7-1200 G2 automation system meets the requirements and protection targets of the following regulations and related amendments:

- Electromagnetic Compatibility Regulations 2016 (EMC)
- Radio Equipment Regulations 2017
- Equipment and Protective Systems Intended for use in Potentially Explosive Atmospheres Regulations 2016 (ATEX)
- Regulations on the restriction of the use of certain hazardous substances in electrical and electronic equipment 2012 (RoHS)
- Supply of Machinery (Safety) Regulations 2008 for S7-1200 G2 F-CPU, F-SM, and F-SB modules

UK Declarations of Conformity for the respective authorities are available from:

Siemens AG
Digital Industries
Factory Automation
P.O. Box 1963
D-92209 Amberg

The UK Declaration of Conformity is also available for download from the Siemens Industry Online Support Web site (<https://sieportal.siemens.com/en-ww/support>) under the keyword "Declaration of Conformity".

cULus approval



Underwriters Laboratories Inc. complying with:

- Underwriters Laboratories, Inc.: UL 61010-1, Safety Requirements for Electrical Equipment for Measurement, Control, and Laboratory Use; Part 1: General Requirements and UL 61010-2-201, Safety Requirements for Electrical Equipment for Measurement, Control, and Laboratory Use - Part 2-201: Particular Requirements for Control Equipment.
- Canadian Standards Association: CAN/CSA-C22.2 No. 61010-1-12, Safety Requirements for Electrical Equipment for Measurement, Control, and Laboratory Use - Part 1: General Requirements and CSA C22.2 No. 61010-2-201, Safety Requirements for Electrical Equipment for Measurement, Control, and Laboratory Use - Part 2-201: Particular Requirements for Control Equipment.

NOTE

The SIMATIC S7-1200 G2 series meets the CSA standard.

The cULus logo indicates that the S7-1200 G2 has been examined and certified by Underwriters Laboratories (UL) to the standards referenced above.

cULus HAZ. LOC. approval



Underwriters Laboratories Inc. in accordance with:

- UL 121201
- CAN/CSA C22.2 No. 213 (Hazardous Location) APPROVED for use in Class I, Division 2, Group A, B, C, D T4C; Class I, Zone 2, Group IIC T4 Installation Instructions for cULus haz.loc.
- WARNING – Explosion Hazard – Do not disconnect while circuit is live unless area is known to be non-hazardous.
- WARNING – Explosion Hazard – Substitution of components can impair suitability for Class I, Division 2 or Zone 2.
- This equipment is suitable for use in Class I, Division 2, Groups A, B, C, D; Class I, Zone 2, Group IIC; or non-hazardous locations.

IMPORTANT EXCEPTION: Some models are de-rated for $T_a = 60\text{ }^{\circ}\text{C}$. See the Technical Specifications of each device for derating information.

ATEX approval



According to EN 60079-7 (Electrical apparatus for potentially explosive atmospheres – Part 7: Increased safety “e”), EN IEC 60079-0 (Electrical apparatus for potentially explosive gas atmospheres – Part 0: General requirements), and IEC 60079-15 (Electrical apparatus for potentially explosive atmospheres - Part 15: Equipment protection by type of protection “n”).

II 3 G Ex ec IIC T4 Gc (some models are II 3 G Ex ec nC IIC T4 Gc, see product marking) (Page 368)

UL 24 ATEX 3237X

Special conditions of use:

- The equipment shall only be used in an area of not more than pollution degree 2, as defined in EN 60664-1.
- The equipment shall be installed in an enclosure that provides a degree of protection not less than IP54 in accordance with EN 60079-7.
- Transient protection shall be provided that is set at a level not exceeding 140% of the peak rated voltage value at the supply terminals to the equipment.

IECEx approval



According to IEC 60079-7 (Explosive atmospheres – Part 7: Equipment protection by increased safety “e”), IEC 60079-0 (Explosive atmospheres – Part 0: Equipment – General requirements), and IEC 60079-15 (Electrical apparatus for potentially explosive atmospheres - Part 15: Equipment protection by type of protection “n”).

II 3 G Ex ec IIC T4 Gc (some models are II 3 G Ex ec nC IIC T4 Gc, see product marking) (Page 368)

IECEx UL 24.0044X

Specific conditions of use:

- The equipment shall only be used in an area of not more than pollution degree 2, as defined in IEC 60664-1.
- The equipment shall be installed in an enclosure that provides a degree of protection not less than IP54 in accordance with EN IEC 60079-0.
- Transient protection shall be provided that is set at a level not exceeding 140% of the peak rated voltage value at the supply terminals to the equipment.

UKEX approval



According to EN 60079-7 (Explosive atmospheres – Part 7: Equipment protection by increased safety “e”), EN IEC 60079-0 (Explosive atmospheres – Part 0: Equipment – General requirements), and IEC 60079-15 (Electrical apparatus for potentially explosive atmospheres - Part 15: Equipment protection by type of protection “n”).

II 3 G Ex ec IIC T4 Gc (some models are II 3 G Ex ec nC IIC T4 Gc, see product marking) ([Page 368](#))

UL 24UKEX2991X

Specific conditions of use:

- The equipment shall only be used in an area of not more than pollution degree 2, as defined in EN 60664-1.
- The equipment shall be installed in an enclosure that provides a degree of protection not less than IP54 in accordance with EN 60079-7.
- Transient protection shall be provided that is set at a level not exceeding 140% of the peak rated voltage value at the supply terminals to the equipment.

CCCEX approval



According to GB/T 3836.1 (Explosive atmospheres – Part 1: Equipment – General requirements), GB/T 3836.3 (Explosive atmospheres – Part 3: Equipment protection by increased safety “e”), and GB/T 3836.8 (Explosive atmospheres – Part 8: Equipment protection by type of protection “n” see product marking) ([Page 368](#))

Specific conditions of safety use:

- The equipment shall only be used in an area of at least pollution degree 2, as defined in GB/T 16935.1.
- The equipment shall be installed in an enclosure that provides a degree of protection not less than IP54 in accordance with GB/T 3836.3.
- Transient protection shall be provided that is set at a level not exceeding 140% of the peak rated voltage value at the supply terminals to the equipment.

Australia and New Zealand - RCM Mark (Regulatory Compliance Mark)



The S7-1200 G2 automation system satisfies the requirements of AS/NZS 2064 standards (Class A).

Korea Certification



The S7-1200 G2 automation system satisfies the requirements of the Korean Certification (KC Mark). It has been defined as Class A Equipment and is intended for industrial applications and has not been considered for home use.

Eurasian Customs Union approval



EAC (Eurasian Conformity): Declaration of Conformity according to Technical Regulation of Customs Union (TR CU)

Industrial environments

The S7-1200 G2 automation system is designed for use in industrial environments.

Table A-1 Industrial environments

Application field	Emission requirements	Immunity requirements
Industrial	EN 61000-6-4	EN 61000-6-2

Environmental conditions

The S7-1200 G2 automation system is suitable for use in weather-proof, fixed locations. The operating conditions are based on requirements of IEC 61131-2:2017.

Table A-2 Shipping and storage

Environmental conditions – Shipping and storage conditions (TTH4 and STH4)	
EN 60068-2-1, Test Ab, Cold EN 60068-2-2, Test Dc, Dry heat	-40 °C to 70 °C
EN 60068-2-30, Test Db, Damp heat	25 °C to 55 °C, 95% RH
EN 60068-2-14, Test Na, Temperature shock	-40 °C to 70 °C, dwell time 3 hours, 2 cycles
EN 60068-2-31, Free fall	0.3 m, 5 times, product packaging
Atmospheric pressure	1140 to 540 hPa (corresponding to an altitude of -1000 to 5000 m)

Table A-3 Climatic ambient conditions

Environmental conditions – Climatic ambient operating conditions (OTH4)	
Ambient temperature (Inlet Air 25 mm below unit)	-20 °C to 40 °C Max. specifications ¹ -20 °C to 60 °C With derating ² For vertical mounting see individual device specifications. Minimum temperature for fail-safe SMs/SBs is 0 °C.

¹ Operating temperature range using maximum voltages and maximum specifications.

² Operating temperature range using the rated voltages, 50% of maximum specifications with alternate I/O active:

50% of maximum specifications includes half of the following values with alternate I/O active:

- Current available for expansion devices
- Current available on sensor supply
- Current for the digital outputs (includes relay outputs)

Alternate I/O active means that every other input or output is active. Using alternate I/O reduces the concentration of heat around active circuits. Refer to the specifications of your CPU for the number of supported inputs and outputs.

A.1 General technical specifications

Environmental conditions – Climatic ambient operating conditions (OTH4)	
Ambient temperature (Inlet Air 25 mm below unit)	95% non-condensing humidity
Atmospheric pressure	1140 to 540 hPa (corresponding to an altitude from -1000 to 5000 m) For altitudes above 2000 m, the maximum permissible ambient temperature must be derated: >2000 m 0.9 factor, >3000 m 0.8 factor, >4000 m 0.7 factor. 5000 m is max allowed altitude.
Effects on the availability of modules at altitude	The higher cosmic radiation present during operation at altitudes above 2000 m affects the failure rate of electronic components. This is what is called a soft-error rate. In rare cases, this can result in a transition of modules to the safe state, especially for fail-safe modules. However, the functional safety of the modules is fully retained.
Concentration of contaminants	SO ₂ : < 0.5 ppm; H ₂ S: < 0.1 ppm; RH < 60% non-condensing
	ISA-S71.04 severity level G1, G2, G3
EN 60068-2-14, Test Nb (Temperature change)	-20 °C to 60 °C, dwell time 3 hours, 5 cycles
EN 60068-2-78, Test Cab (Damp heat)	30 °C, 95% RH, 16 hours
EN 60068-2-27 (Shock)	15 g, 11 ms pulse, 6 shocks in each of 3 axes (when panel mounted)
EN 60068-2-6 (Sinusoidal vibration)	3.5 mm from 5 to 8.4 Hz, 1g from 8.4 to 150 Hz 10 sweeps each axis, 1 octave per minute (when panel or DIN rail mounted) Note: In high vibration applications, Siemens recommends panel mounting or the use of a Siemens DIN Rail with DIN Rail End Retainers to secure devices.

¹ Operating temperature range using maximum voltages and maximum specifications.

² Operating temperature range using the rated voltages, 50% of maximum specifications with alternate I/O active:

50% of maximum specifications includes half of the following values with alternate I/O active:

- Current available for expansion devices
- Current available on sensor supply
- Current for the digital outputs (includes relay outputs)

Alternate I/O active means that every other input or output is active. Using alternate I/O reduces the concentration of heat around active circuits. Refer to the specifications of your CPU for the number of supported inputs and outputs.

Maximum installation altitude

You can install all S7-1200 G2 devices at a maximum altitude of 5000 m except for the following devices:

Description	Article number	Version	Maximum installation altitude
SM 1222 DQ 16xRLY	6ES7222-5HH50-0XB0	FS01 or higher	4000 m
SM 1223 DI 8x24VDC / DQ 8x RLY	6ES7223-5PH50-0XB0	FS01 or higher	4000 m
SM 1223 DI 16x24VDC / DQ 1-6xRLY	6ES7223-5PL50-0XB0	FS01 or higher	4000 m

Electromagnetic compatibility

Electromagnetic Compatibility (EMC) is the ability of an electrical device to operate as intended in an electromagnetic environment and to operate without emitting levels of electromagnetic interference (EMI) that can disturb other electrical devices in the vicinity.

Table A-4 Immunity

Electromagnetic compatibility - Immunity per EN 61000-6-2	
EN 61000-4-2 ¹ Electrostatic discharge	8 kV air discharge to all surfaces 6 kV contact discharge to exposed conductive surfaces
EN 61000-4-3 ² Radiated, radio-frequency, electromagnetic field immunity test	80 MHz to 1000 MHz, 10 V/m, 80% AM (1 kHz) 1.4 GHz to 6 GHz, 3 V/m, 80% AM (1 kHz)
EN 61000-4-4 ¹ Fast transient bursts	2 kV, 5 kHz with coupling network to AC and DC system power 2 kV, 5 kHz with coupling clamp to I/O
EN 61000-4-5 ¹ Surge immunity	AC systems - 2 kV common mode, 1 kV differential mode DC systems - 1 kV common mode, 0.5 kV differential mode
EN 61000-4-6 ² Conducted disturbances	150 kHz to 80 MHz, 10 V RMS, 80% AM at 1 kHz
EN 61000-4-11 Voltage dips	AC systems 0% for 1 cycle, 40% for 12 cycles, and 70% for 30 cycles at 60 Hz

¹ The maximum short-term influence on analog modules during the duration of the EMC tests can be +/- 10% of the full-scale value.

² The maximum short-term influence on analog modules during the duration of the EMC tests can be +/- 1% of the full-scale value.

Table A-5 Emissions

Electromagnetic compatibility - Conducted and radiated emissions per EN 61000-6-4		
Conducted emissions AC power ports	0.15 MHz to 0.5 MHz	< 79 dBμV quasi-peak, < 66 dBμV average
	0.5 MHz to 30 MHz	< 73 dBμV quasi-peak, < 60 dBμV average
Conducted emissions DC power ports	0.15 MHz to 0.5 MHz	< 89 dBμV quasi-peak, < 76 dBμV average
	0.5 MHz to 30 MHz	< 83 dBμV quasi-peak, < 70 dBμV average
Radiated emissions	30 MHz to 230 MHz	< 40 dBμV/m quasi-peak at 10 m

Electromagnetic compatibility - Conducted and radiated emissions per EN 61000-6-4		
Radiated emissions	230 MHz to 1000 MHz	< 47 dB μ V/m quasi-peak at 10 m
	1000 MHz to 3000 MHz	< 76 dB μ V/m peak, < 56 dB μ V/m average at 3 m
	3000 MHz to 6000 MHz	< 80 dB μ V/m peak, < 60 dB μ V/m average at 3 m

Insulation

The insulation is designed in accordance with the requirements of IEC 61010-2-201.

NOTE

For modules having 24 V DC (SELV / PELV) supply voltage, galvanic isolations are tested with 707 V DC (type test).

Pollution degree / overvoltage category in accordance with IEC 61131-2 and IEC 61010-2-201

- Pollution degree 2
- Overvoltage category II

Protection class according to IEC 61131-2 and IEC 61010-2-201

- Protection class II

Degree of protection

- IP20 Mechanical Protection, EN 60529
- Protects against finger contact with high voltage as tested by standard probe. External protection required for dust, dirt, water and foreign objects of < 12.5 mm in diameter.

Rated voltages

The rated voltages are:

- 24 V DC
- 120/240 V AC

WARNING

Risks when turning on output power

When a mechanical contact turns on output power to the S7-1200 G2 CPU, or any digital expansion module or board, it sends a "1" signal to the digital outputs for approximately 50 microseconds.

This could cause unexpected machine or process operation, which could result in death or serious injury to personnel and/or damage to equipment.

You must plan for the "1" signal to the digital outputs.

Reverse voltage protection

Reverse voltage protection circuitry is provided on each terminal pair of +24 V DC power or user input power for CPUs, signal modules (SMs), and signal boards (SBs). It is still possible to damage the system by wiring different terminal pairs in opposite polarities.

Some of the 24 V DC power input ports in the S7-1200 G2 system are interconnected, with a common logic circuit connecting multiple M terminals. For example, the following circuits are interconnected when designated as "not isolated": the 24 V DC power supply of the CPU, the sensor power of the CPU, the power input for the relay coil of an SM, and the power supply for a non-isolated analog input. All non-isolated M terminals must connect to the same external reference potential.

WARNING

Risks when connecting non-isolated M terminals to different reference potentials

Connecting non-isolated M terminals to different reference potentials causes unintended current flows that can cause damage or unpredictable operation in the PLC and any connected equipment.

Always ensure that all non-isolated M terminals in an S7-1200 G2 system are connected to the same reference potential.

Failure to comply with these guidelines could cause damage or unpredictable operation, which can result in death or severe personal injury and/or property damage.

DC Outputs

Short-circuit protection circuitry is not provided for DC outputs on CPUs, signal modules (SMs), and signal boards (SBs).

Relay electrical service life

The typical performance data estimated from sample tests is shown below. Actual performance can vary depending upon your specific application. An external protection circuit that is adapted to the load enhances the service life of the contacts. Normally closed contacts have a typical service life of about one-third that of normally open contacts under inductive and lamp load conditions.

Table A-6 Typical performance data

Data for selecting an actuator			
Continuous thermal current		2 A max.	
Switching capacity and life of the contacts			
For ohmic load	Voltage	Current	Number of operating cycles (typical)
	24 V DC	2.0 A	0.1 million
	24 V DC	1.0 A	0.2 million
	24 V DC	0.5 A	1.0 million
	48 V AC	1.5 A	1.5 million
	60 V AC	1.5 A	1.5 million
	120 V AC	2.0 A	1.0 million
	120 V AC	1.0 A	1.5 million
	120 V AC	0.5 A	2.0 million
	230 V AC	2.0 A	1.0 million
	230 V AC	1.0 A	1.5 million
	230 V AC	0.5 A	2.0 million
For inductive load (according to IEC 947-5-1 DC13/AC15)	Voltage	Current	Number of operating cycles (typical)
	24 V DC	2.0 A	0.05 million
	24 V DC	1.0 A	0.1 million
	24 V DC	0.5 A	0.5 million
	24 V AC	1.5 A	1.0 million
	48 V AC	1.5 A	1.0 million
	60 V AC	1.5 A	1.0 million
	120 V AC	2.0 A	0.7 million
	120 V AC	1.0 A	1.0 million
	120 V AC	0.5 A	1.5 million
	230 V AC	2.0 A	0.7 million
	230 V AC	1.0 A	1.0 million
230 V AC	0.5 A	1.5 million	
Activating a digital input		Possible	
Switching frequency			
Mechanical		Max. 10 Hz	

Data for selecting an actuator	
At ohmic load	Max. 1 Hz
At inductive load (according to IEC 947-5-1 DC13/AC15)	Max. 0.5 Hz
At lamp load	Max. 1Hz

Internal CPU memory retention

The CPU performs operations to extend the life of the internal memory devices that contain the application data. Below is the life expectancy of the internal memory.

- Lifetime of retentive data and data log data: 10 years
- Power down retentive data, write cycle endurance: 2 million cycles
- Data log data, write cycle endurance: 500 million data log entries

NOTE

Effect of data logs on internal CPU memory

Each data log write consumes at a minimum 2 KB of memory. If your program writes small amounts of data frequently, it is consuming at least 2 KB of memory on each write. A better implementation would be to accumulate the small data items in a data block (DB), and to write the data block to the data log at less frequent intervals.

If your program writes many data log entries at a high frequency, consider using a replaceable SD memory card.

Use of cellular phones

You can read information from the CPU and write operations to the CPU from the passive Near Field Communication (NFC) [\(Page 315\)](#) tag in your S7-1200 G2 CPU by placing your iPhone near the NFC symbol on the CPU.

All S7-1200 G2 CPUs and modules have a scannable QR code lasered on the housing. Use your smartphone's camera to read the QR code. The QR code provides a direct link to the Siemens Industrial Online Support information for your device.

 WARNING Risks when using a cellular phone in close proximity to the S7-1200 G2 CPU Using a cellular phone in close proximity to an S7-1200 G2 system with cellular and Wi-Fi communications active can cause unpredictable behavior. To reduce any influence of a cellular phone on the S7-1200 G2 system, and to ensure proper operation of your CPU, place the phone in "Airplane mode" to disable cellular and Wi-Fi before bringing the phone into proximity (<10 cm) of the CPU. Failure to comply with these guidelines can cause damage or unpredictable operation which could result in severe personal injury, property damage, and/or death.

⚠ WARNING Risks when operating a cellular phone in a hazardous or explosive environment Do not use a cellular phone in a hazardous or explosive environment unless the phone has been approved for use in such environments. Failure to comply with these guidelines can cause damage or unpredictable operation which could result in severe personal injury, property damage, and/or death.

A.2 Protection methods

The S7-1200 G2 automation system is covered by two protection methods:

Article numbers covered by II 3 G Ex ec IIC T4 Gc / Ex ec IIC T4 Gc	Article numbers covered by II 3 G Ex ec nC IIC T4 Gc / Ex ec nC IIC T4 Gc
6ES7212-1AG50-0XB0	6ES7212-1HG50-0XB0
6ES7214-1AH50-0XB0	6ES7212-1BG50-0XB0
6ES7212-1AF50-0XB0	6ES7214-1HH50-0XB0
6ES7214-1AF50-0XB0	6ES7214-1BH50-0XB0
6ES7221-1BH50-0XB0	6ES7212-1HF50-0XB0
6ES7222-5BH50-0XB0	6ES7214-1HF50-0XB0
6ES7223-5BH50-0XB0	6ES7222-5HH50-0XB0
6ES7232-4HF50-0XB0	6ES7223-5PH50-0XB0
6ES7221-3BF50-0XB0	6ES7231-4HF50-0XB0
6ES7222-5BF50-0XB0	6ES7233-4HF50-0XB0
6ES7223-7BF50-0XB0	6ES7231-4HD50-0XB0
6ES7223-7AF50-0XB0	6ES7233-4HD50-0XB0
6ES7232-4HD50-0XB0	6ES7223-5PL50-0XB0
6ES7231-5QF50-0XB0	
6ES7231-5PD50-0XB0	
6ES7241-1EA50-0XB0	
6ES7231-5QD50-0XB0	
6ES7231-5PB50-0XB0	
6ES7241-1CA50-0XB0	
6ES7223-5BL50-0XB0	
6ES7223-5BL50-1XB0	
6ES7297-4AX50-0XA0	
6ES7226-6ME50-0XB0	

A.3 CPU 1212C

A.3.1 General specifications and features

Table A-7 General

Technical data	CPU 1212C AC/DC/RLY	CPU 1212C DC/DC/RLY	CPU 1212C DC/DC/DC
Article number	6ES7212-1BG50-0XB0	6ES7212-1HG50-0XB0	6ES7212-1AG50-0XB0
Dimensions W x H x D	70 x 125 x 100 mm		
Weight (product/shipping)	373 grams / 420 grams	333 grams / 380 grams	319 grams / 366 grams
Power dissipation	4.0 W	3.0 W	
Current available for expansion devices	1000 mA max. (5 V DC)		
Current available on sensor supply	300 mA (24 V DC sensor power, current limited)		
Operating environment	Horizontal mounting -20 °C to 40 °C ¹ -20 °C to 60 °C ²		
	Vertical mounting -20 °C to 50 °C ²		Vertical mounting -20 °C to 40 °C ¹ -20 °C to 50 °C ²
	95% relative humidity at 25 °C during operation, without condensation, maximum		

¹ Operating temperature range using maximum voltages and maximum specifications

² Operating temperature range using rated voltages, 50% of maximum specifications, and alternate I/O active

Table A-8 CPU features

Technical data	Description	
User memory	Work Memory	150 Kbytes (Program) 500 Kbytes (Data)
	Load Memory	8 Mbytes (Internal) 32 Gbytes (using SD card)
	Retentive Memory	20 Kbytes
Onboard digital I/O	8 inputs / 6 outputs	
Process image size	1024 bytes of inputs (I) / 1024 bytes of outputs (Q)	
Bit memory size	8192 bytes (M)	
Temporary (local) memory	Per priority class, max.	64 Kbytes
	Per block, max.	16 Kbytes
Communication module/processor expansion	3 max. (must connect to the right of the CPU or to the right of another CM/CP)	
Signal module expansion (SM plus CM)	6 max.	
Signal board or Communication board expansion	1 max.	
High-speed counters	Max. number of high-speed counters	8 (any CPU or SB digital input)

¹ For CPU models with relay outputs, you must install a signal board (SB) containing DC digital outputs to use the pulse outputs.

Technical data	Description	
High-speed counters	Max. rate, CPU inputs Ia.0 to Ia.5	100 kHz (80 kHz in quadrature mode)
	Max. rate, CPU inputs Ia.6 to Ia.7	30 kHz (20 kHz in quadrature mode)
	Max. rate, SB inputs	See SB specifications
Pulse outputs ¹	Max. number of pulse outputs	8 (any CPU or SB digital output)
	Max. rate, CPU outputs Qa.0 to Qa.3	100 kHz
	Max. rate, CPU outputs Qa.4 to Qa.5	20 kHz
	Max. rate, SB outputs	See SB specifications
Pulse catch inputs	Yes, each onboard CPU digital input and SB digital input	
Time delay interrupts	20 total with 1 ms resolution	
Cyclic interrupts	20 total with 1 µs resolution	
Edge interrupts	Rising and falling for each onboard CPU digital input and SB digital input	
Memory card (Page 500)	SIMATIC memory card (optional).	
Motion control	Available Resources	800
	Required Resources	40 per speed-controlled axis
		80 per positioning axis
		160 per synchronous axis
		80 per external encoder
		20 per output cam
		160 per cam track
		40 per measuring input
	Available Extended Resources	40
PID	PID Compact	Yes, universal PID controller with integrated optimization
	PID 3Step	Yes, PID controller with integrated optimization for valves
	PID Temp	Yes, PID controller with integrated optimization for temperature
Real-time clock	Accuracy	+/- 60 seconds per month
	Retention time, super capacitor	20 days typical at 40 °C, 12 days minimum at 40 °C

¹ For CPU models with relay outputs, you must install a signal board (SB) containing DC digital outputs to use the pulse outputs.

A.3.2 Performance

Table A-9 Performance

Type of instruction ¹	Direct addressing (I, Q, and M)	DB accesses
Boolean	0.037 µs/instruction	
Move_Bool	0.067 µs/instruction	0.066 µs/instruction
Move_Word	0.027 µs/instruction	0.030 µs/instruction
Move_Real	0.027 µs/instruction	0.030 µs/instruction
Add_Real	0.119 µs/instruction	0.074 µs/instruction

¹ Many variables affect measured times. The above performance times are for the fastest instructions in each category and error-free programs.

A.3.3 Blocks, timers, and counters

Table A-10 Blocks, times, and counters

Element	Description	
Blocks	Type	OB, FB, FC, DB
	Max. number of elements	4000; Blocks (OB, FB, FC, DB) and UDTs
	Max. OB, FB, FC size	64 Kbytes
	Max. DB size (Optimized)	500 Kbytes Work Memory 16 Mbytes Load Memory
	Max. DB size (Non-optimized)	64 Kbytes (DBs with absolute addressing)
	Address range for FBs and FCs	1 to 65535
	Address range for DBs	1 to 59999
	Nesting depth per priority class ¹	24 (OB plus 23 more levels)
	Monitoring	Status of 8 code blocks can be monitored simultaneously.
Number of OBs per event class	Program cycle	100
	Startup	100
	Time delay interrupt	20 (one per event)
	Cyclic interrupt	20 (one per event)
	Hardware interrupt	50
	Time error interrupt	1
	Diagnostic error interrupt	1
	Pull or plug of modules	1
	Rack or station failure	1
	Time of day	20 (one per event)
	Synchronous Cycle	1
	Status	1
	Update	1
	Profile	1

¹ Safety programs use 2 nesting levels; the user program, therefore, has a nesting depth of 22 in safety programs.

Element	Description	
Number of OBs per event class	MC-Interpolator	1
	MC-Servo	1
	MC-PreServo	1
	MC-PostServo	1
	MC-LookAhead	1
	MC-PreInterpolator	1
	Programming error	1
	I/O access error	1
Timers	Type	IEC
	Quantity	Limited only by memory size
	Storage	Structure in DB, size depends upon time type
	IEC_TIMER	16 bytes
	IEC_LTIMER	28 bytes
Counters	Type	IEC
	Quantity	Limited only by memory size
	Storage	Structure in DB, size depends upon count type
	IEC_SCOUNTER, IEC_USCOUNTER	3 bytes
	IEC_COUNTER, IEC_UCOUNTER	6 bytes
	IEC_DCOUNTER, IEC_UDCOUNTER	12 bytes
	IEC_LCOUNTER, IEC_ULCOUNTER	24 bytes
Runtime Meters	Quantity	16

¹ Safety programs use 2 nesting levels; the user program, therefore, has a nesting depth of 22 in safety programs.

A.3.4 Communications

Table A-11 Communications

Technical data	Description
Number of ports	2 with an integrated switch
Type	Ethernet (RJ-45 connector)
Connections	88 connections max. (integrated into CPU) 10 reserved for ES/HMI/web
Data rates	100 Mb/s
Isolation (Page 84) (external signal to logic)	Transformer isolated, 1500 V AC (type test) ¹
Cable type	CAT5e shielded
Interfaces	1 PROFINET
	0 PROFIBUS

¹ Ethernet port isolation limits hazards during short term network faults to hazardous voltages. It does not conform to safety requirements for routine AC line voltage isolation.

Technical data	Description	
PROFINET Protocols	PROFINET IO controller	Yes
	PROFINET IO device	Yes
	SIMATIC communication	Yes
	Open IE communication	Yes
	Web server	Yes
	Media redundancy	Yes
PROFINET IO controller services	PG/OP communication	Yes
	S7 routing	Yes (requires more than one communication interface)
	Isochronous mode	Yes
	Open IE communication	Yes
	IRT	Yes
	MRP	Yes
	MRPD	Yes – Requires an IRT sync domain
	PROFenergy	Yes (per user program)
	Prioritized startup	Yes (max. 16 PROFINET devices)
	Number of connectable I/O devices, max.	31 (30 if I-Device is used, 29 if shared I-Device is used)
	Number of submodules, max.	512
	Number of IO devices that you can connect for RT, max.	31 (30 if I-Device is used, 29 if shared I-Device is used)
	Number of in line IO devices that you can connect for RT, max.	31
	Number of IO devices that you can connect for IRT, max.	31 (30 if I-Device is used, 29 if shared I-Device is used)
	Number of IO devices that can be activated/deactivated simultaneously, max.	8
	The minimum update time depends on the communication component set for PROFINET IO, on the number of IO devices, and the quantity of configured user data.	RT Send clock: 1 ms to 512 ms IRT Send clock: 1 ms to 512 ms (1 ms resolution)
PROFINET I-Device	Number of connections, max.	2
PROFINET I-Device services	PG/OP communication	Yes
	S7 routing	No
	Isochronous mode	No
	Open IE communication	Yes
	IRT	Yes
	MRP	Yes
	PROFenergy	Yes (per user program)
	Shared device	Yes

¹ Ethernet port isolation limits hazards during short term network faults to hazardous voltages. It does not conform to safety requirements for routine AC line voltage isolation.

Technical data	Description	
PROFINET I-Device services	Number of IO controllers with shared device, max.	2
SIMATIC communication	S7 communication as server	Yes
	S7 communication as client	Yes
	User data per job, max.	See TIA Portal information system (S7 communication, user data size)
Open IE communication	TCP/IP	Yes, 64 Kbytes max. data length Several passive connections per port
	ISO-on-TCP (RFC1006)	Yes, 64 Kbytes max. data length
	UDP	Yes, 2048 bytes max. data length 1472 bytes max. for UDP broadcast
	DHCP	Yes
	SNMP	Yes
	DCP	Yes
	LLDP	Yes
Near Field Communication (NFC)	Yes, with the S7-1200 G2 NFC app	
S7 message functions	Number of login stations for message functions, max.	32
	Program alarms	Yes
	Number of configurable program messages, max.	5000
	Number of loadable program messages in RUN, max.	2500
	Number of simultaneously active program alarms	600 program alarms 100 alarms for system diagnostics 160 for motion technology objects
Test commissioning functions	Joint commission (Team Engineering)	Yes, parallel online access possible for up to 5 engineering systems
	Program status	Yes, up to 8 blocks simultaneously (in total across all ES clients)
	Single step	No
	Breakpoints	No
	SIMATIC Controller Profiling	Yes
Monitor/modify	Variables	Inputs/outputs, memory bits, DBs, distributed I/Os, timers, counters
	Number of monitor variables, max.	200 per job
	Number of modify variables, max.	200 per job
Force	Variables	Peripheral inputs/outputs
	Number of variables, max.	200
Trace	Number of configurable traces	4
	Variables captured per trace, max.	16

¹ Ethernet port isolation limits hazards during short term network faults to hazardous voltages. It does not conform to safety requirements for routine AC line voltage isolation.

Technical data	Description	
Trace	Data captured per trace, max.	512 KB
Diagnostics buffer	Number of entries, max.	500
	Retentive	100

¹ Ethernet port isolation limits hazards during short term network faults to hazardous voltages. It does not conform to safety requirements for routine AC line voltage isolation.

A.3.5 Power supply and sensor power

Table A-12 Power supply

Technical data	CPU 1212C AC/DC/RLY	CPU 1212C DC/DC/RLY	CPU 1212C DC/DC/DC
Rated voltage	120/240 V AC	24 V DC	
Voltage range	85 to 264 V AC	20.4 to 28.8 V DC	
Reverse voltage protection	--	Yes	
Line frequency	47 to 63 Hz	--	
Input current (CPU only)	70 mA at 120 V AC 38 mA at 240 V AC	185 mA at 24 V DC	125 mA at 24 V DC
Input current (with all accessories)	330 mA at 120 V AC 200 mA at 240 V AC	765 mA at 24 V DC	700 mA at 24 V DC
Inrush current	20 A max. at 264 V AC	12 A max. at 28.8 V DC	
I ² t	0.8 A ² s	0.5 A ² s	
Isolation (input power to logic)	1500 V AC	Not isolated	
Ground leakage (AC line to func- tional earth)	0.5 mA max.	--	
Hold up time (loss of power)	20 ms at 120 V AC 80 ms at 240 V AC	10 ms at 24 V DC	
Internal fuse	3 A, 250 V, slow blow not user replaceable		

Table A-13 Sensor power

Technical data	CPU 1212C AC/DC/RLY	CPU 1212C DC/DC/RLY	CPU 1212C DC/DC/DC
Rated voltage	24 V DC		
Voltage range	20.4 to 28.8 V DC	L+ minus 4 V DC min.	
Output current rating	300 mA max. (short-circuit protected)		
Ripple noise (<10 MHz)	< 1 V peak to peak max.	Same as input line	
Isolation (CPU logic to sensor power)	Not isolated		
Cable length	500 m shielded		
Cable size	0.2 mm² to 1.5 mm² (AWG 24 to 16)		

A.3.6 Digital inputs and outputs

Table A-14 Digital inputs

Technical data	CPU 1212C AC/DC/RLY	CPU 1212C DC/DC/RLY	CPU 1212C DC/DC/DC
Number of inputs	8, in 1 isolation group of 8 inputs		
Assignment	Ia.0 to Ia.5 (high-speed) Ia.6 to Ia.7 (standard)		
Type	Sink/Source (IEC Type 1 sink)		
Rated voltage	24 V DC at 6 mA, nominal (high-speed) 24 V DC at 4 mA, nominal (standard)		
Continuous permissible voltage	30 V DC, max. at 8 mA, max. (high-speed) 30 V DC, max. at 6 mA, max. (standard)		
Logic 1 signal	15 V DC min. at 2.5 mA		
Logic 0 signal	5 V DC max. or 0.5 mA		
Isolation (field side to logic)	707 V DC (type test)		
Filter times (selectable by channel)	μ s settings: 0.1, 0.2, 0.4, 0.8, 1.6, 3.2, 6.4, 10.0, 12.8, 20.0 ms settings: 0.05, 0.1, 0.2, 0.4, 0.8, 1.6, 3.2, 6.4, 10.0, 12.8, 20.0		
HSC clock input rates (Logic 1 level = 15 to 30 V DC)	Single phase: 100 kHz (Ia.0 to Ia.5) Single phase: 30 kHz (Ia.6 to Ia.7) Quadrature phase: 80 kHz (Ia.0 to Ia.5) Quadrature phase: 20 kHz (Ia.6 to Ia.7)		
Cable length	500 m shielded, 300 m unshielded, 50 m shielded for HSC inputs		
Cable size	0.2 mm ² to 1.5 mm ² (AWG 24 to 16)		

Table A-15 Digital outputs

Technical data	CPU 1212C AC/DC/RLY	CPU 1212C DC/DC/RLY	CPU 1212C DC/DC/DC
Number of outputs	6, in 1 isolation group of 6 outputs		
Assignment	Qa.0 to Qa.5		Qa.0 to Qa.3 (high-speed) Qa.4 to Qa.5 (standard)
Type	Relay, dry contact		Solid state – MOSFET (sourcing)
Rated voltage	--		24 V DC
Voltage range	5 to 30 V DC or 5 to 250 V AC		20.4 to 28.8 V DC
Logic 1 signal at max. current	--		20 V DC min.
Logic 0 signal with 10 k Ω load	--		0.1 V DC max.
Current	2.0 A max.		0.5 A max.
Minimum load ¹	125 mW DC / 500 mW AC		--
Lamp load	30 W DC / 200 W AC		5 W
ON state resistance	0.2 Ω max. when new		0.6 Ω max.

¹ When using relays at minimum load, avoid ambient temperatures below 0 °C.

² For CPU models with relay outputs, you must install a signal board (SB) containing DC digital outputs to use the pulse outputs.

³ Depending on your pulse receiver and cable, an additional load resistor (at least 10% of rated current) can improve pulse signal quality and noise immunity.

Technical data	CPU 1212C AC/DC/RLY	CPU 1212C DC/DC/RLY	CPU 1212C DC/DC/DC
Leakage current per point	--		10 µA max.
Overload protection	No		
Isolation (field side to logic)	1500 V AC (type test)		707 V DC (type test)
Isolation (coil to logic)	None		--
Current per common	12 A max. (10 A max. per pin)		3 A max.
Inductive clamp voltage	--		L+ minus 40 V, 1 W dissipation
Switching delay (Qa.0 to Qa.3)	10 ms max.		1.0 µs max., OFF to ON 3.0 µs max., ON to OFF
Switching delay (Qa.4 to Qa.5)	10 ms max.		5 µs max., OFF to ON 20 µs max., ON to OFF
Maximum relay switching frequency	1 Hz		--
Pulse Train Output (PTO) rate	Not recommended ²		100 kHz max. (Qa.0 to Qa.3) 20 kHz max. (Qa.4 to Qa.5) 2 Hz min. ³
Lifetime mechanical (no load)	10000000 open/close cycles		--
Lifetime contacts at rated load	100000 open/close cycles		--
Behavior on RUN to STOP	Last value or substitute value (default value 0)		
Control of a digital input	Yes		
Parallel outputs for redundant load control	Yes (with same common)		
Parallel outputs for increased load	No		
Cable length	500 m shielded, 150 m unshielded		
Cable size	0.2 mm ² to 1.5 mm ² (AWG 24 to 16)		

¹ When using relays at minimum load, avoid ambient temperatures below 0 °C.

² For CPU models with relay outputs, you must install a signal board (SB) containing DC digital outputs to use the pulse outputs.

³ Depending on your pulse receiver and cable, an additional load resistor (at least 10% of rated current) can improve pulse signal quality and noise immunity.

A.3.7 Wiring diagrams

The wiring diagrams and pin connector locations are shown below:

CPU 1212C AC/DC/RLY

① For additional noise immunity, jumper the Sensor Power "M" to Chassis Ground on the connector.

② For sinking inputs, connect "-" to "M" (shown). For sourcing inputs, connect "+" to "M".

X80: AC power wiring terminal (Orange, Type-A keying)					
AC power	L1		N		
Pin #	1	3	5		
Pin #	2	4	6		
Sensor power	GND	L+	M		
X10: DC input wiring terminal (Gray, No keying)					
Signal	DI a.0	DI a.1	DI a.2	DI a.3	DI a.4
Pin #	1	3	5	7	9
Pin #	2	4	6	8	10
Signal	DI a.5	DI a.6	DI a.7	1M	1M
X11: Relay output wiring terminal (Orange, Type-A keying)					
Signal	1L	DQ a.0	DQ a.1	DQ a.2	
Pin #	1	3	5	7	
Pin #	2	4	6	8	
Signal	1L	DQ a.3	DQ a.4	DQ a.5	

NOTE

You can connect either the L1 or N (L2) terminal to a voltage source up to 240 V AC. The N terminal can be considered L2 and is not required to be grounded. No polarization is required for L1 and N (L2) terminals.

CPU 1212C DC/DC/RLY

① For additional noise immunity, jumper the 24 V DC Power "M" to Chassis Ground on the connector.

② For sinking inputs, connect "-" to "M" (shown). For sourcing inputs, connect "+" to "M".

X80: DC power wiring terminal (Gray, No keying)				
DC power	L+		M	
Pin #	1	3	5	
Pin #	2	4	6	
Sensor power	GND	L+	M	

CPU 1212C DC/DC/RLY

		X10: DC input wiring terminal (Gray, No keying)					
		Signal	DI a.0	DI a.1	DI a.2	DI a.3	DI a.4
		Pin #	1	3	5	7	9
		Pin #	2	4	6	8	10
		Signal	DI a.5	DI a.6	DI a.7	1M	1M
		X11: Relay output wiring terminal (Orange, Type-A keying)					
		Signal	1L	DQ a.0	DQ a.1	DQ a.2	
		Pin #	1	3	5	7	
		Pin #	2	4	6	8	
		Signal	1L	DQ a.3	DQ a.4	DQ a.5	

① For additional noise immunity, jumper the 24 V DC Power "M" to Chassis Ground on the connector.

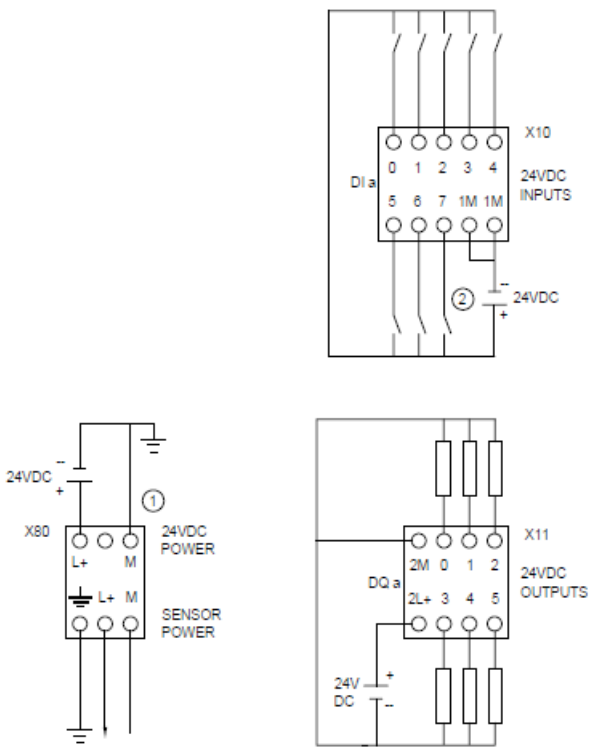
② For sinking inputs, connect "-" to "M" (shown). For sourcing inputs, connect "+" to "M".

CPU 1212C DC/DC/DC

		X80: DC power wiring terminal (Gray, No keying)					
		DC power	L+		M		
		Pin #	1	3	5		
		Pin #	2	4	6		
		Sensor power	GND	L+	M		
		X10: DC input wiring terminal (Gray, No keying)					
		Signal	DI a.0	DI a.1	DI a.2	DI a.3	DI a.4
		Pin #	1	3	5	7	9
		Pin #	2	4	6	8	10
		Signal	DI a.5	DI a.6	DI a.7	1M	1M
		X11: DC output wiring terminal (Gray, No keying)					

① For additional noise immunity, jumper the 24 V DC Power "M" to Chassis Ground on the connector.

② For sinking inputs, connect "-" to "M" (shown). For sourcing inputs, connect "+" to "M".

CPU 1212C DC/DC/DC					
	Signal	2M	DQ a.0	DQ a.1	DQ a.2
	Pin #	1	3	5	7
	Pin #	2	4	6	8
	Signal	2L+	DQ a.3	DQ a.4	DQ a.5

① For additional noise immunity, jumper the 24 V DC Power "M" to Chassis Ground on the connector.

② For sinking inputs, connect "-" to "M" (shown). For sourcing inputs, connect "+" to "M".

A.4 CPU 1212FC

A.4.1 General specifications and features

Table A-16 General

Technical data	CPU 1212FC DC/DC/RLY	CPU 1212FC DC/DC/DC
Article number	6ES7212-1HF50-0XB0	6ES7212-1AF50-0XB0
Dimensions W x H x D	70 x 125 x 100 mm	
Weight (product/shipping)	333 grams / 380 grams	319 grams / 366 grams
Power dissipation	3.0 W	
Current available for expansion devices	1000 mA max. (5 V DC)	
Current available on sensor supply	300 mA (24 V DC sensor power, current limited)	

¹ Operating temperature range using maximum voltages and maximum specifications

² Operating temperature range using rated voltages, 50% of maximum specifications, and alternate I/O active

Technical data	CPU 1212FC DC/DC/RLY	CPU 1212FC DC/DC/DC
Safety class (highest)	PL e (performance level according to ISO 13849-1) SIL 3 (safety integrity level according to IEC 61508)	
Probability of failure	Low demand mode: PFDavg in accordance with SIL 3 < 2.00E-05 High demand/continuous mode: PFH in accordance with SIL 3 < 1.00E-09 (altitude -1000 m to 3000 m) < 2.00E-09 (altitude >3000 m to 5000 m) For service life of 20 years and repair time of 100 hours	
Operating environment	Horizontal mounting -20 °C to 40 °C ¹ -20 °C to 60 °C ²	
	Vertical mounting -20 °C to 50 °C ²	Vertical mounting -20 °C to 40 °C ¹ -20 °C to 50 °C ²
	95% relative humidity at 25 °C during operation, without condensation, maximum	

¹ Operating temperature range using maximum voltages and maximum specifications

² Operating temperature range using rated voltages, 50% of maximum specifications, and alternate I/O active

Table A-17 CPU features

Technical data	Description	
User memory	Work Memory	200 Kbytes (Program) 500 Kbytes (Data)
	Load Memory	8 Mbytes (Internal) 32 Gbytes (using SD card)
	Retentive Memory	20 Kbytes
Onboard digital I/O	8 inputs / 6 outputs	
Process image size	1024 bytes of inputs (I) / 1024 bytes of outputs (Q)	
Bit memory size	8192 bytes (M)	
Temporary (local) memory	Per priority class, max.	64 Kbytes
	Per block, max.	16 Kbytes
Communication module/processor expansion	3 max. (must connect to the right of the CPU or to the right of another CM/CP)	
Signal module expansion (SM plus CM)	6 max.	
Signal board or Communication board expansion	1 max.	
High-speed counters	Max. number of high-speed counters	8 (any CPU or SB digital input)
	Max. rate, CPU inputs Ia.0 to Ia.5	100 kHz (80 kHz in quadrature mode)
	Max. rate, CPU inputs Ia.6 to Ia.7	30 kHz (20 kHz in quadrature mode)
	Max. rate, SB inputs	See SB specifications
Pulse outputs ¹	Max. number of pulse outputs	8 (any CPU or SB digital output)

¹ For CPU models with relay outputs, you must install a signal board (SB) containing DC digital outputs to use the pulse outputs.

A.4 CPU 1212FC

Technical data	Description	
Pulse outputs ¹	Max. rate, CPU outputs Qa.0 to Qa.3	100 kHz
	Max. rate, CPU outputs Qa.4 to Qa.5	20 kHz
	Max. rate, SB outputs	See SB specifications
Pulse catch inputs	Yes, each onboard CPU digital input and SB digital input	
Time delay interrupts	20 total with 1 ms resolution	
Cyclic interrupts	20 total with 1 µs resolution	
Edge interrupts	Rising and falling for each onboard CPU digital input and SB digital input	
Memory card (Page 500)	SIMATIC memory card (optional).	
Motion control	Available Resources	800
	Required Resources	40 per speed-controlled axis
		80 per positioning axis
		160 per synchronous axis
		80 per external encoder
		20 per output cam
		160 per cam track
		40 per measuring input
	Available Extended Resources	40
PID	PID Compact	Yes, universal PID controller with integrated optimization
	PID 3Step	Yes, PID controller with integrated optimization for valves
	PID Temp	Yes, PID controller with integrated optimization for temperature
Real-time clock	Accuracy	+/- 60 seconds per month
	Retention time, super capacitor	20 days typical at 40 °C, 12 days minimum at 40 °C

¹ For CPU models with relay outputs, you must install a signal board (SB) containing DC digital outputs to use the pulse outputs.

A.4.2 Performance

Table A-18 Performance

Type of instruction ¹	Direct addressing (I, Q, and M)	DB accesses
Boolean	0.037 µs/instruction	
Move_Bool	0.067 µs/instruction	0.066 µs/instruction
Move_Word	0.027 µs/instruction	0.030 µs/instruction
Move_Real	0.027 µs/instruction	0.030 µs/instruction
Add_Real	0.119 µs/instruction	0.074 µs/instruction

¹ Many variables affect measured times. The above performance times are for the fastest instructions in each category and error-free programs.

A.4.3 Blocks, timers, and counters

Table A-19 Blocks, times, and counters

Element	Description	
Blocks	Type	OB, FB, FC, DB
	Max. number of elements	4000; Blocks (OB, FB, FC, DB) and UDTs
	Max. OB, FB, FC size	64 Kbytes
	Max. DB size (Optimized)	500 Kbytes Work Memory 16 Mbytes Load Memory
	Max. DB size (Non-optimized)	64 Kbytes (DBs with absolute addressing)
	Address range for FBs and FCs	1 to 65535
	Address range for DBs	1 to 59999
	Nesting depth per priority class ¹	24 (OB plus 23 more levels)
	Monitoring	Status of 8 code blocks can be monitored simultaneously.
Number of OBs per event class	Program cycle	100
	Startup	100
	Time delay interrupt	20 (one per event)
	Cyclic interrupt	20 (one per event)
	Hardware interrupt	50
	Time error interrupt	1
	Diagnostic error interrupt	1
	Pull or plug of modules	1
	Rack or station failure	1
	Time of day	20 (one per event)
	Synchronous Cycle	1
	Status	1
	Update	1
	Profile	1

¹ Safety programs use 2 nesting levels; the user program, therefore, has a nesting depth of 22 in safety programs.

Element	Description	
Number of OBs per event class	MC-Interpolator	1
	MC-Servo	1
	MC-PreServo	1
	MC-PostServo	1
	MC-LookAhead	1
	MC-PreInterpolator	1
	Programming error	1
	I/O access error	1
Timers	Type	IEC
	Quantity	Limited only by memory size
	Storage	Structure in DB, size depends upon time type
	IEC_TIMER	16 bytes
	IEC_LTIMER	28 bytes
Counters	Type	IEC
	Quantity	Limited only by memory size
	Storage	Structure in DB, size depends upon count type
	IEC_SCOUNTER, IEC_USCOUNTER	3 bytes
	IEC_COUNTER, IEC_UCOUNTER	6 bytes
	IEC_DCOUNTER, IEC_UDCOUNTER	12 bytes
	IEC_LCOUNTER, IEC_ULCOUNTER	24 bytes
Runtime Meters	Quantity	16

¹ Safety programs use 2 nesting levels; the user program, therefore, has a nesting depth of 22 in safety programs.

A.4.4 Communications

Table A-20 Communications

Technical data	Description
Number of ports	2 with an integrated switch
Type	Ethernet (RJ-45 connector)
Connections	88 connections max. (integrated into CPU) 10 reserved for ES/HMI/web
Data rates	100 Mb/s
Isolation (Page 84) (external signal to logic)	Transformer isolated, 1500 V AC (type test) ¹
Cable type	CAT5e shielded
Interfaces	1 PROFINET
	0 PROFIBUS

¹ Ethernet port isolation limits hazards during short term network faults to hazardous voltages. It does not conform to safety requirements for routine AC line voltage isolation.

Technical data	Description	
PROFINET Protocols	PROFINET IO controller	Yes
	PROFINET IO device	Yes
	SIMATIC communication	Yes
	Open IE communication	Yes
	Web server	Yes
	Media redundancy	Yes
PROFINET IO controller services	PG/OP communication	Yes
	S7 routing	Yes (requires more than one communication interface)
	Isochronous mode	Yes
	Open IE communication	Yes
	IRT	Yes
	MRP	Yes
	MRPD	Yes – Requires an IRT sync domain
	PROFenergy	Yes (per user program)
	Prioritized startup	Yes (max. 16 PROFINET devices)
	Number of connectable I/O devices, max.	31 (30 if I-Device is used, 29 if shared I-Device is used)
	Number of submodules, max.	512
	Number of IO devices that you can connect for RT, max.	31 (30 if I-Device is used, 29 if shared I-Device is used)
	Number of in line IO devices that you can connect for RT, max.	31
	Number of IO devices that you can connect for IRT, max.	31 (30 if I-Device is used, 29 if shared I-Device is used)
	Number of IO devices that can be activated/deactivated simultaneously, max.	8
	The minimum update time depends on the communication component set for PROFINET IO, on the number of IO devices, and the quantity of configured user data.	RT Send clock: 1 ms to 512 ms IRT Send clock: 1 ms to 512 ms (1 ms resolution)
PROFINET I-Device	Number of connections, max.	2
PROFINET I-Device services	PG/OP communication	Yes
	S7 routing	No
	Isochronous mode	No
	Open IE communication	Yes
	IRT	Yes
	MRP	Yes
	PROFenergy	Yes (per user program)
	Shared device	Yes

¹ Ethernet port isolation limits hazards during short term network faults to hazardous voltages. It does not conform to safety requirements for routine AC line voltage isolation.

Technical data	Description	
PROFINET I-Device services	Number of IO controllers with shared device, max.	2
SIMATIC communication	S7 communication as server	Yes
	S7 communication as client	Yes
	User data per job, max.	See TIA Portal information system (S7 communication, user data size)
Open IE communication	TCP/IP	Yes, 64 Kbytes max. data length Several passive connections per port
	ISO-on-TCP (RFC1006)	Yes, 64 Kbytes max. data length
	UDP	Yes, 2048 bytes max. data length 1472 bytes max. for UDP broadcast
	DHCP	Yes
	SNMP	Yes
	DCP	Yes
	LLDP	Yes
Near Field Communication (NFC)	Yes, with the S7-1200 G2 NFC app	
S7 message functions	Number of login stations for message functions, max.	32
	Program alarms	Yes
	Number of configurable program messages, max.	5000
	Number of loadable program messages in RUN, max.	2500
	Number of simultaneously active program alarms	600 program alarms 100 alarms for system diagnostics 160 for motion technology objects
Test commissioning functions	Joint commission (Team Engineering)	Yes, parallel online access possible for up to 5 engineering systems
	Program status	Yes, up to 8 blocks simultaneously (in total across all ES clients)
	Single step	No
	Breakpoints	No
	SIMATIC Controller Profiling	Yes
Monitor/modify	Variables	Inputs/outputs, memory bits, DBs, distributed I/Os, timers, counters
	Number of monitor variables, max.	200 per job
	Number of modify variables, max.	200 per job
Force	Variables	Peripheral inputs/outputs
	Number of variables, max.	200
Trace	Number of configurable traces	4
	Variables captured per trace, max.	16

¹ Ethernet port isolation limits hazards during short term network faults to hazardous voltages. It does not conform to safety requirements for routine AC line voltage isolation.

Technical data	Description	
Trace	Data captured per trace, max.	512 KB
Diagnostics buffer	Number of entries, max.	500
	Retentive	100

¹ Ethernet port isolation limits hazards during short term network faults to hazardous voltages. It does not conform to safety requirements for routine AC line voltage isolation.

A.4.5 Power supply and sensor power

Table A-21 Power supply

Technical data	CPU 1212FC DC/DC/RLY	CPU 1212FC DC/DC/DC
Rated voltage	24 V DC	
Voltage range	20.4 to 28.8 V DC	
Reverse voltage protection	Yes	
Input current (CPU only)	185 mA at 24 V DC	125 mA at 24 V DC
Input current (with all accessories)	765 mA at 24 V DC	700 mA at 24 V DC
Inrush current	12 A max. at 28.8 V DC	
I ² t	0.5 A ² s	
Isolation (input power to logic)	Not isolated	
Hold up time (loss of power)	10 ms at 24 V DC	
Internal fuse	3 A, 250 V, slow blow not user replaceable	

Table A-22 Sensor power

Technical data	CPU 1212FC DC/DC/RLY	CPU 1212FC DC/DC/DC
Rated voltage	24 V DC	
Voltage range	L+ minus 4 V DC min.	
Output current rating	300 mA max. (short-circuit protected)	
Ripple noise (<10 MHz)	Same as input line	
Isolation (CPU logic to sensor power)	Not isolated	
Cable length	500 m shielded	
Cable size	0.2 mm ² to 1.5 mm ² (AWG 24 to 16)	

A.4.6 Digital inputs and outputs

Table A-23 Digital inputs

Technical data	CPU 1212FC DC/DC/RLY	CPU 1212FC DC/DC/DC
Number of inputs	8, in 1 isolation group of 8 inputs	
Assignment	Ia.0 to Ia.5 (high-speed) Ia.6 to Ia.7 (standard)	
Type	Sink/Source (IEC Type 1 sink)	
Rated voltage	24 V DC at 6 mA, nominal (high-speed) 24 V DC at 4 mA, nominal (standard)	
Continuous permissible voltage	30 V DC, max. at 8 mA, max. (high-speed) 30 V DC, max. at 6 mA, max. (standard)	
Logic 1 signal	15 V DC min. at 2.5 mA	
Logic 0 signal	5 V DC max. or 0.5 mA	
Isolation (field side to logic)	707 V DC (type test)	
Filter times (selectable by channel)	μs settings: 0.1, 0.2, 0.4, 0.8, 1.6, 3.2, 6.4, 10.0, 12.8, 20.0 ms settings: 0.05, 0.1, 0.2, 0.4, 0.8, 1.6, 3.2, 6.4, 10.0, 12.8, 20.0	
HSC clock input rates (Logic 1 level = 15 to 30 V DC)	Single phase: 100 kHz (Ia.0 to Ia.5) Single phase: 30 kHz (Ia.6 to Ia.7) Quadrature phase: 80 kHz (Ia.0 to Ia.5) Quadrature phase: 20 kHz (Ia.6 to Ia.7)	
Cable length	500 m shielded, 300 m unshielded, 50 m shielded for HSC inputs	
Cable size	0.2 mm ² to 1.5 mm ² (AWG 24 to 16)	

Table A-24 Digital outputs

Technical data	CPU 1212FC DC/DC/RLY	CPU 1212FC DC/DC/DC
Number of outputs	6, in 1 isolation group of 6 outputs	
Assignment	Qa.0 to Qa.5	Qa.0 to Qa.3 (high-speed) Qa.4 to Qa.5 (standard)
Type	Relay, dry contact	Solid state – MOSFET (sourcing)
Rated voltage	--	24 V DC
Voltage range	5 to 30 V DC or 5 to 250 V AC	20.4 to 28.8 V DC
Logic 1 signal at max. current	--	20 V DC min.
Logic 0 signal with 10 kΩ load	--	0.1 V DC max.
Current	2.0 A max.	0.5 A max.
Minimum load ¹	125 mW DC / 500 mW AC	--
Lamp load	30 W DC / 200 W AC	5 W
ON state resistance	0.2 Ω max. when new	0.6 Ω max.

¹ When using relays at minimum load, avoid ambient temperatures below 0 °C.

² For CPU models with relay outputs, you must install a signal board (SB) containing DC digital outputs to use the pulse outputs.

³ Depending on your pulse receiver and cable, an additional load resistor (at least 10% of rated current) can improve pulse signal quality and noise immunity.

Technical data	CPU 1212FC DC/DC/RLY	CPU 1212FC DC/DC/DC
Leakage current per point	--	10 µA max.
Overload protection	No	
Isolation (field side to logic)	1500 V AC (type test)	707 V DC (type test)
Isolation (coil to logic)	None	--
Current per common	12 A max. (10 A max. per pin)	3 A max.
Inductive clamp voltage	--	L+ minus 40 V, 1 W dissipation
Switching delay (Qa.0 to Qa.3)	10 ms max.	1.0 µs max., OFF to ON 3.0 µs max., ON to OFF
Switching delay (Qa.4 to Qa.5)	10 ms max.	5 µs max., OFF to ON 20 µs max., ON to OFF
Maximum relay switching frequency	1 Hz	--
Pulse Train Output (PTO) rate	Not recommended ²	100 kHz max. (Qa.0 to Qa.3) 20 kHz max. (Qa.4 to Qa.5) 2 Hz min. ³
Lifetime mechanical (no load)	10000000 open/close cycles	--
Lifetime contacts at rated load	100000 open/close cycles	--
Behavior on RUN to STOP	Last value or substitute value (default value 0)	
Control of a digital input	Yes	
Parallel outputs for redundant load control	Yes (with same common)	
Parallel outputs for increased load	No	
Cable length	500 m shielded, 150 m unshielded	
Cable size	0.2 mm ² to 1.5 mm ² (AWG 24 to 16)	

¹ When using relays at minimum load, avoid ambient temperatures below 0 °C.

² For CPU models with relay outputs, you must install a signal board (SB) containing DC digital outputs to use the pulse outputs.

³ Depending on your pulse receiver and cable, an additional load resistor (at least 10% of rated current) can improve pulse signal quality and noise immunity.

A.4.7 Wiring diagrams

The wiring diagrams and pin connector locations are shown below:

CPU 1212FC DC/DC/RLY

① For additional noise immunity, jumper the 24 V DC Power "M" to Chassis Ground on the connector.

② For sinking inputs, connect "-" to "M" (shown). For sourcing inputs, connect "+" to "M".

CPU 1212FC DC/DC/DC

X80: DC power wiring terminal (Gray, No keying)						
DC power	L+		M			
Pin #	1	3	5			
Pin #	2	4	6			
Sensor power	GND	L+	M			
X10: DC input wiring terminal (Gray, No keying)						
Signal	DI a.0	DI a.1	DI a.2	DI a.3	DI a.4	
Pin #	1	3	5	7	9	
Pin #	2	4	6	8	10	

① For additional noise immunity, jumper the 24 V DC Power "M" to Chassis Ground on the connector.

② For sinking inputs, connect "-" to "M" (shown). For sourcing inputs, connect "+" to "M".

CPU 1212FC DC/DC/DC						
				Signal	DI a.5	DI a.6
				Signal	DI a.7	1M
				X11: DC output wiring terminal (Gray, No keying)		
				Signal	2M	DQ a.0
				Pin #	1	3
				Pin #	2	4
				Signal	2L+	DQ a.3
						DQ a.4
						DQ a.5

① For additional noise immunity, jumper the 24 V DC Power "M" to Chassis Ground on the connector.

② For sinking inputs, connect "-" to "M" (shown). For sourcing inputs, connect "+" to "M".

A.5 CPU 1214C

A.5.1 General specifications and features

Table A-25 General

Technical data	CPU 1214C AC/DC/RLY	CPU 1214C DC/DC/RLY	CPU 1214C DC/DC/DC
Article number	6ES7214-1BH50-0XB0	6ES7214-1HH50-0XB0	6ES7214-1AH50-0XB0
Dimensions W x H x D	80 x 125 x 100 mm		
Weight (product/shipping)	417 grams / 474 grams	376 grams / 433 grams	352 grams / 409 grams
Power dissipation	4.0 W	3.5 W	
Current available for expansion devices	1600 mA max. (5 V DC)		
Current available on sensor supply	400 mA (24 V DC sensor power, current limited)		

¹ Operating temperature range using maximum voltages and maximum specifications

² Operating temperature range using rated voltages, 50% of maximum specifications, and alternate I/O active

A.5 CPU 1214C

Technical data	CPU 1214C AC/DC/RLY	CPU 1214C DC/DC/RLY	CPU 1214C DC/DC/DC
Operating environment	Horizontal mounting -20 °C to 40 °C ¹ -20 °C to 60 °C ²		
	Vertical mounting -20 °C to 50 °C ²		Vertical mounting -20 °C to 40 °C ¹ -20 °C to 50 °C ²
	95% relative humidity at 25 °C during operation, without condensation, maximum		

¹ Operating temperature range using maximum voltages and maximum specifications

² Operating temperature range using rated voltages, 50% of maximum specifications, and alternate I/O active

Table A-26 CPU features

Technical data	Description	
User memory	Work Memory	250 Kbytes (Program) 750 Kbytes (Data)
	Load Memory	8 Mbytes (Internal) 32 Gbytes (using SD card)
	Retentive Memory	20 Kbytes
Onboard digital I/O	14 inputs / 10 outputs	
Process image size	1024 bytes of inputs (I) / 1024 bytes of outputs (Q)	
Bit memory size	8192 bytes (M)	
Temporary (local) memory	Per priority class, max.	64 Kbytes
	Per block, max.	16 Kbytes
Communication module/processor expansion	3 max. (must connect to the right of the CPU or to the right of another CM/CP)	
Signal module expansion (SM plus CM)	10 max.	
Signal board or Communication board expansion	2 max.	
High-speed counters	Max. number of high-speed counters	8 (any CPU or SB digital input)
	Max. rate, CPU inputs Ia.0 to Ia.5	100 kHz (80 kHz in quadrature mode)
	Max. rate, CPU inputs Ia.6 to Ib.5	30 kHz (20 kHz in quadrature mode)
	Max. rate, SB inputs	See SB specifications
Pulse outputs ¹	Max. number of pulse outputs	8 (any CPU or SB digital output)
	Max. rate, CPU outputs Qa.0 to Qa.3	100 kHz
	Max. rate, CPU outputs Qa.4 to Qb.1	20 kHz
	Max. rate, SB outputs	See SB specifications
Pulse catch inputs	Yes, each onboard CPU digital input and SB digital input	
Time delay interrupts	20 total with 1 ms resolution	
Cyclic interrupts	20 total with 1 µs resolution	
Edge interrupts	Rising and falling for each onboard CPU digital input and SB digital input	

¹ For CPU models with relay outputs, you must install a signal board (SB) containing DC digital outputs to use the pulse outputs.

Technical data	Description	
Memory card (Page 500)	SIMATIC memory card (optional).	
Motion control	Available Resources	800
	Required Resources	40 per speed-controlled axis
		80 per positioning axis
		160 per synchronous axis
		80 per external encoder
		20 per output cam
		160 per cam track
		40 per measuring input
PID	Available Extended Resources	40
	Required Extended Resources	2 per cam (1000 points)
		30 for each set of kinematics
PID	PID Compact	Yes, universal PID controller with integrated optimization
	PID 3Step	Yes, PID controller with integrated optimization for valves
	PID Temp	Yes, PID controller with integrated optimization for temperature
Real-time clock	Accuracy	+/- 60 seconds per month
	Retention time, super capacitor	20 days typical at 40 °C, 12 days minimum at 40 °C

¹ For CPU models with relay outputs, you must install a signal board (SB) containing DC digital outputs to use the pulse outputs.

A.5.2 Performance

Table A-27 Performance

Type of instruction ¹	Direct addressing (I, Q, and M)	DB accesses
Boolean	0.037 µs/instruction	
Move_Bool	0.067 µs/instruction	0.066 µs/instruction
Move_Word	0.027 µs/instruction	0.030 µs/instruction
Move_Real	0.027 µs/instruction	0.030 µs/instruction
Add_Real	0.119 µs/instruction	0.074 µs/instruction

¹ Many variables affect measured times. The above performance times are for the fastest instructions in each category and error-free programs.

A.5.3 Blocks, timers, and counters

Table A-28 Blocks, times, and counters

Element	Description	
Blocks	Type	OB, FB, FC, DB
	Max. number of elements	4000; Blocks (OB, FB, FC, DB) and UDTs
	Max. OB, FB, FC size	64 Kbytes
	Max. DB size (Optimized)	750 Kbytes Work Memory 16 Mbytes Load Memory
	Max. DB size (Non-optimized)	64 Kbytes (DBs with absolute addressing)
	Address range for FBs and FCs	1 to 65535
	Address range for DBs	1 to 59999
	Nesting depth per priority class ¹	24 (OB plus 23 more levels)
	Monitoring	Status of 8 code blocks can be monitored simultaneously.
Number of OBs per event class	Program cycle	100
	Startup	100
	Time delay interrupt	20 (one per event)
	Cyclic interrupt	20 (one per event)
	Hardware interrupt	50
	Time error interrupt	1
	Diagnostic error interrupt	1
	Pull or plug of modules	1
	Rack or station failure	1
	Time of day	20 (one per event)
	Synchronous Cycle	1
	Status	1
	Update	1
	Profile	1
	MC-Interpolator	1
	MC-Servo	1
	MC-PreServo	1
	MC-PostServo	1
	MC-LookAhead	1
	MC-PreInterpolator	1
	Programming error	1
	I/O access error	1
Timers	Type	IEC
	Quantity	Limited only by memory size
	Storage	Structure in DB, size depends upon time type

¹ Safety programs use 2 nesting levels; the user program, therefore, has a nesting depth of 22 in safety programs.

Element	Description	
Timers	IEC_TIMER	16 bytes
	IEC_LTIMER	28 bytes
Counters	Type	IEC
	Quantity	Limited only by memory size
	Storage	Structure in DB, size depends upon count type
	IEC_SCOUNTER, IEC_USCOUNTER	3 bytes
	IEC_COUNTER, IEC_UCOUNTER	6 bytes
	IEC_DCOUNTER, IEC_UDCOUNTER	12 bytes
	IEC_LCOUNTER, IEC_ULCOUNTER	24 bytes
Runtime Meters	Quantity	16

¹ Safety programs use 2 nesting levels; the user program, therefore, has a nesting depth of 22 in safety programs.

A.5.4 Communications

Table A-29 Communications

Technical data	Description	
Number of ports	2 with an integrated switch	
Type	Ethernet (RJ-45 connector)	
Connections	88 connections max. (integrated into CPU) 10 reserved for ES/HMI/web	
Data rates	100 Mb/s	
Isolation (Page 84) (external signal to logic)	Transformer isolated, 1500 V AC (type test) ¹	
Cable type	CAT5e shielded	
Interfaces	1 PROFINET	
	0 PROFIBUS	
PROFINET Protocols	PROFINET IO controller	Yes
	PROFINET IO device	Yes
	SIMATIC communication	Yes
	Open IE communication	Yes
	Web server	Yes
	Media redundancy	Yes
PROFINET IO controller services	PG/OP communication	Yes
	S7 routing	Yes (requires more than one communication interface)
	Isochronous mode	Yes
	Open IE communication	Yes
	IRT	Yes

¹ Ethernet port isolation limits hazards during short term network faults to hazardous voltages. It does not conform to safety requirements for routine AC line voltage isolation.

Technical data	Description	
PROFINET IO controller services	MRP	Yes
	MRPD	Yes – Requires an IRT sync domain
	PROFenergy	Yes (per user program)
	Prioritized startup	Yes (max. 16 PROFINET devices)
	Number of connectable I/O devices, max.	31 (30 if I-Device is used, 29 if shared I-Device is used)
	Number of submodules, max.	512
	Number of IO devices that you can connect for RT, max.	31 (30 if I-Device is used, 29 if shared I-Device is used)
	Number of in line IO devices that you can connect for RT, max.	31
	Number of IO devices that you can connect for IRT, max.	31 (30 if I-Device is used, 29 if shared I-Device is used)
	Number of IO devices that can be activated/deactivated simultaneously, max.	8
	The minimum update time depends on the communication component set for PROFINET IO, on the number of IO devices, and the quantity of configured user data.	RT Send clock: 1 ms to 512 ms IRT Send clock: 1 ms to 512 ms (1 ms resolution)
PROFINET I-Device	Number of connections, max.	2
PROFINET I-Device services	PG/OP communication	Yes
	S7 routing	No
	Isochronous mode	No
	Open IE communication	Yes
	IRT	Yes
	MRP	Yes
	PROFenergy	Yes (per user program)
	Shared device	Yes
	Number of IO controllers with shared device, max.	2
SIMATIC communication	S7 communication as server	Yes
	S7 communication as client	Yes
	User data per job, max.	See TIA Portal information system (S7 communication, user data size)
Open IE communication	TCP/IP	Yes, 64 Kbytes max. data length Several passive connections per port
	ISO-on-TCP (RFC1006)	Yes, 64 Kbytes max. data length
	UDP	Yes, 2048 bytes max. data length 1472 bytes max. for UDP broadcast
	DHCP	Yes
	SNMP	Yes

¹ Ethernet port isolation limits hazards during short term network faults to hazardous voltages. It does not conform to safety requirements for routine AC line voltage isolation.

Technical data	Description	
Open IE communication	DCP	Yes
	LLDP	Yes
Near Field Communication (NFC)	Yes, with the S7-1200 G2 NFC app	
S7 message functions	Number of login stations for message functions, max.	32
	Program alarms	Yes
	Number of configurable program messages, max.	5000
	Number of loadable program messages in RUN, max.	2500
	Number of simultaneously active program alarms	600 program alarms 100 alarms for system diagnostics 160 for motion technology objects
Test commissioning functions	Joint commission (Team Engineering)	Yes, parallel online access possible for up to 5 engineering systems
	Program status	Yes, up to 8 blocks simultaneously (in total across all ES clients)
	Single step	No
	Breakpoints	No
	SIMATIC Controller Profiling	Yes
Monitor/modify	Variables	Inputs/outputs, memory bits, DBs, distributed I/Os, timers, counters
	Number of monitor variables, max.	200 per job
	Number of modify variables, max.	200 per job
Force	Variables	Peripheral inputs/outputs
	Number of variables, max.	200
Trace	Number of configurable traces	4
	Variables captured per trace, max.	16
	Data captured per trace, max.	512 KB
Diagnostics buffer	Number of entries, max.	500
	Retentive	100

¹ Ethernet port isolation limits hazards during short term network faults to hazardous voltages. It does not conform to safety requirements for routine AC line voltage isolation.

A.5.5 Power supply and sensor power

Table A-30 Power supply

Technical data	CPU 1214C AC/DC/RLY	CPU 1214C DC/DC/RLY	CPU 1214C DC/DC/DC
Rated voltage	120/240 V AC	24 V DC	
Voltage range	85 to 264 V AC	20.4 to 28.8 V DC	
Reverse voltage protection	--	Yes	
Line frequency	47 to 63 Hz	--	
Input current (CPU only)	80 mA at 120 V AC 44 mA at 240 V AC	245 mA at 24 V DC	145 mA at 24 V DC
Input current (with all accessories)	480 mA at 120 V AC 275 mA at 240 V AC	1100 mA at 24 V DC	1000 mA at 24 V DC
Inrush current	20 A max. at 264 V AC	12 A max. at 28.8 V DC	
I ² t	0.8 A ² s	0.5 A ² s	
Isolation (input power to logic)	1500 V AC	Not isolated	
Ground leakage (AC line to functional earth)	0.5 mA max.	--	
Hold up time (loss of power)	20 ms at 120 V AC 80 ms at 240 V AC	10 ms at 24 V DC	
Internal fuse	3 A, 250 V, slow blow not user replaceable		

Table A-31 Sensor power

Technical data	CPU 1214C AC/DC/RLY	CPU 1214C DC/DC/RLY	CPU 1214C DC/DC/DC
Rated voltage	24 V DC		
Voltage range	20.4 to 28.8 V DC	L+ minus 4 V DC min.	
Output current rating	400 mA max. (short-circuit protected)		
Ripple noise (<10 MHz)	< 1 V peak to peak max.	Same as input line	
Isolation (CPU logic to sensor power)	Not isolated		
Cable length	500 m shielded		
Cable size	0.2 mm ² to 1.5 mm ² (AWG 24 to 16)		

A.5.6 Digital inputs and outputs

Table A-32 Digital inputs

Technical data	CPU 1214C AC/DC/RLY	CPU 1214C DC/DC/RLY	CPU 1214C DC/DC/DC
Number of inputs	14, in 1 isolation group of 14 inputs		
Assignment	Ia.0 to Ia.5 (high-speed) Ia.6 to Ib.5 (standard)		
Type	Sink/Source (IEC Type 1 sink)		
Rated voltage	24 V DC at 6 mA, nominal (high-speed) 24 V DC at 4 mA, nominal (standard)		
Continuous permissible voltage	30 V DC, max. at 8 mA, max. (high-speed) 30 V DC, max. at 6 mA, max. (standard)		
Logic 1 signal	15 V DC min. at 2.5 mA		
Logic 0 signal	5 V DC max. or 0.5 mA		
Isolation (field side to logic)	707 V DC (type test)		
Current per common	20 A mix. (10 A max. per pin)		5 A max.
Filter times (selectable by channel)	µs settings: 0.1, 0.2, 0.4, 0.8, 1.6, 3.2, 6.4, 10.0, 12.8, 20.0 ms settings: 0.05, 0.1, 0.2, 0.4, 0.8, 1.6, 3.2, 6.4, 10.0, 12.8, 20.0		
HSC clock input rates (Logic 1 level = 15 to 30 V DC)	Single phase: 100 kHz (Ia.0 to Ia.5) Single phase: 30 kHz (Ia.6 to Ib.5) Quadrature phase: 80 kHz (Ia.0 to Ia.5) Quadrature phase: 20 kHz (Ia.6 to Ib.5)		
Cable length	500 m shielded, 300 m unshielded, 50 m shielded for HSC inputs		
Cable size	0.2 mm ² to 1.5 mm ² (AWG 24 to 16)		

Table A-33 Digital outputs

Technical data	CPU 1214C AC/DC/RLY	CPU 1214C DC/DC/RLY	CPU 1214C DC/DC/DC
Number of outputs	10, in 1 isolation group of 10 outputs		
Assignment	Qa.0 to Qb.1		Qa.0 to Qa.3 (high-speed) Qa.4 to Qb.1 (standard)
Type	Relay, dry contact		Solid state – MOSFET (sourcing)
Rated voltage	--		24 V DC
Voltage range	5 to 30 V DC or 5 to 250 V AC		20.4 to 28.8 V DC
Logic 1 signal at max. current	--		20 V DC min.
Logic 0 signal with 10 kΩ load	--		0.1 V DC max.
Current	2.0 A max.		0.5 A max.
Minimum load ¹	125 mW DC / 500 mW AC		--
Lamp load	30 W DC / 200 W AC		5 W

¹ When using relays at minimum load, avoid ambient temperatures below 0 °C.

² For CPU models with relay outputs, you must install a signal board (SB) containing DC digital outputs to use the pulse outputs.

³ Depending on your pulse receiver and cable, an additional load resistor (at least 10% of rated current) can improve pulse signal quality and noise immunity.

A.5 CPU 1214C

Technical data	CPU 1214C AC/DC/RLY	CPU 1214C DC/DC/RLY	CPU 1214C DC/DC/DC
ON state resistance	0.2 Ω max. when new		0.6 Ω max.
Leakage current per point	--		10 μ A max.
Overload protection	No		
Isolation (field side to logic)	1500 V AC (type test)		707 V DC (type test)
Isolation (coil to logic)	None		--
Current per common	20 A max. (10 A. max. per pin)		5 A. max.
Inductive clamp voltage	--		L+ minus 40 V, 1 W dissipation
Switching delay (Qa.0 to Qa.3)	10 ms max.		1.0 μ s max., OFF to ON 3.0 μ s max., ON to OFF
Switching delay (Qa.4 to Qb.1)	10 ms max.		5 μ s max., OFF to ON 20 μ s max., ON to OFF
Maximum relay switching frequency	1 Hz		--
Pulse Train Output (PTO) rate	Not recommended ²		100 kHz max. (Qa.0 to Qa.3) 20 kHz max. (Qa.4 to Qb.1) 2 Hz min. ³
Lifetime mechanical (no load)	10000000 open/close cycles		--
Lifetime contacts at rated load	100000 open/close cycles		--
Behavior on RUN to STOP	Last value or substitute value (default value 0)		
Control of a digital input	Yes		
Parallel outputs for redundant load control	Yes (with same common)		
Parallel outputs for increased load	No		
Cable length	500 m shielded, 150 m unshielded		
Cable size	0.2 mm ² to 1.5 mm ² (AWG 24 to 16)		

¹ When using relays at minimum load, avoid ambient temperatures below 0 °C.

² For CPU models with relay outputs, you must install a signal board (SB) containing DC digital outputs to use the pulse outputs.

³ Depending on your pulse receiver and cable, an additional load resistor (at least 10% of rated current) can improve pulse signal quality and noise immunity.

A.5.7 Wiring diagrams

The wiring diagrams and pin connector locations are shown below:

CPU 1214C AC/DC/RLY

X80: AC power wiring terminal (Orange, Type-A keying)

AC power	L1		N
Pin #	1	3	5
Pin #	2	4	6
Sensor power	GND	L+	M

X10: DC input wiring terminal (Gray, No keying)

Signal	DI a.0	DI a.1	DI a.2	DI a.3	DI a.4	DI a.5	DI a.6	DI a.7
Pin #	1	3	5	7	9	11	13	15
Pin #	2	4	6	8	10	12	14	16
Signal	DI b.0	DI b.1	DI b.2	DI b.3	DI b.4	DI b.5	1M	1M

X11: Relay output wiring terminal (Orange, Type-A keying)

Signal	1L	DQ a.0	DQ a.1	DQ a.2	DQ a.3	DQ a.4	
Pin #	1	3	5	7	9	11	
Pin #	2	4	6	8	10	12	
Signal	1L	DQ a.5	DQ a.6	DQ a.7	DQ b.0	DQ b.1	

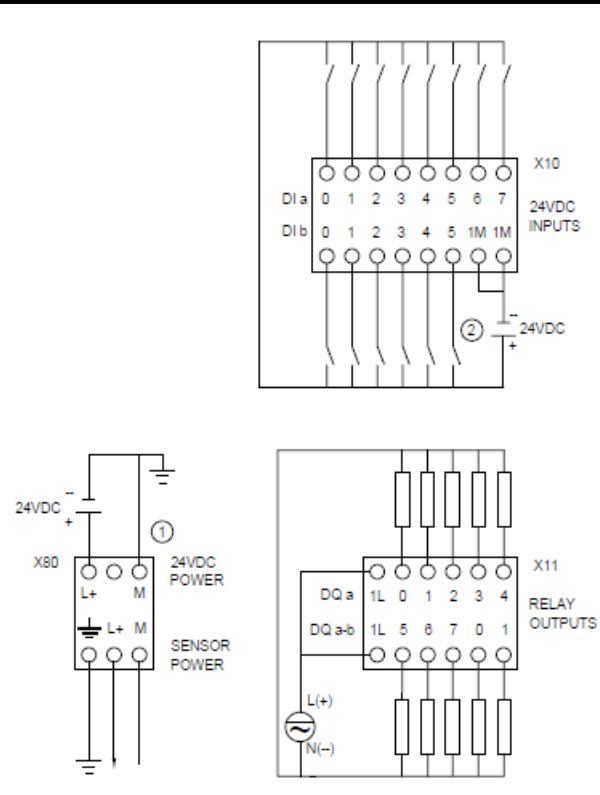
① For additional noise immunity, jumper the Sensor Power "M" to Chassis Ground on the connector.

② For sinking inputs, connect "-" to "M" (shown). For sourcing inputs, connect "+" to "M".

CPU 1214C DC/DC/RLY									
	X80: DC power wiring terminal (Gray, No keying)								
	DC power	L+		M					
	Pin #	1	3	5					
	Pin #	2	4	6					
	Sensor power	GND	L+	M					
	X10: DC input wiring terminal (Gray, No keying)								
	Signal	DI a.0	DI a.1	DI a.2	DI a.3	DI a.4	DI a.5	DI a.6	DI a.7
	Pin #	1	3	5	7	9	11	13	15
	Pin #	2	4	6	8	10	12	14	16

① For additional noise immunity, jumper the 24 V DC Power "M" to Chassis Ground on the connector.

② For sinking inputs, connect "-" to "M" (shown). For sourcing inputs, connect "+" to "M".

CPU 1214C DC/DC/RLY								
	Signal	DI b.0	DI b.1	DI b.2	DI b.3	DI b.4	DI b.5	1M 1M
	X11: Relay output wiring terminal (Orange, Type-A keying)							
	Signal	1L	DQ a.0	DQ a.1	DQ a.2	DQ a.3	DQ a.4	
	Pin #	1	3	5	7	9	11	
	Pin #	2	4	6	8	10	12	
	Signal	1L	DQ a.5	DQ a.6	DQ a.7	DQ b.0	DQ b.1	

- ① For additional noise immunity, jumper the 24 V DC Power "M" to Chassis Ground on the connector.
- ② For sinking inputs, connect "-" to "M" (shown). For sourcing inputs, connect "+" to "M".

CPU 1214C DC/DC/DC								
	X80: DC power wiring terminal (Gray, No keying)							
	DC power	L+		M				
	Pin #	1	3	5				
	Pin #	2	4	6				
	Sensor power	GND	L+	M				
	X10: DC input wiring terminal (Gray, No keying)							
	Signal	DI a.0	DI a.1	DI a.2	DI a.3	DI a.4	DI a.5	DI a.6
	Pin #	1	3	5	7	9	11	13
	Pin #	2	4	6	8	10	12	14
	Signal	DI b.0	DI b.1	DI b.2	DI b.3	DI b.4	DI b.5	1M 1M

- ① For additional noise immunity, jumper the 24 V DC Power "M" to Chassis Ground on the connector.
- ② For sinking inputs, connect "-" to "M" (shown). For sourcing inputs, connect "+" to "M".

CPU 1214C DC/DC/DC							
	Signal	2M	DQ a.0	DQ a.1	DQ a.2	DQ a.3	DQ a.4
	Pin #	1	3	5	7	9	11
	Pin #	2	4	6	8	10	12
	Signal	2L+	DQ a.5	DQ a.6	DQ a.7	DQ b.0	DQ b.1

① For additional noise immunity, jumper the 24 V DC Power "M" to Chassis Ground on the connector.

② For sinking inputs, connect "-" to "M" (shown). For sourcing inputs, connect "+" to "M".

A.6 CPU 1214FC

A.6.1 General specifications and features

Table A-34 General

Technical data	CPU 1214FC DC/DC/RLY	CPU 1214FC DC/DC/DC
Article number	6ES7214-1HF50-0XB0	6ES7214-1AF50-0XB0
Dimensions W x H x D	80 x 125 x 100 mm	
Weight (product/shipping)	376 grams / 433 grams	352 grams / 409 grams
Power dissipation	3.5 W	
Current available for expansion devices	1600 mA max. (5 V DC)	
Current available on sensor supply	400 mA (24 V DC sensor power, current limited)	

¹ Operating temperature range using maximum voltages and maximum specifications

² Operating temperature range using rated voltages, 50% of maximum specifications, and alternate I/O active

A.6 CPU 1214FC

Technical data	CPU 1214FC DC/DC/RLY	CPU 1214FC DC/DC/DC
Safety class (highest)	PL e (performance level according to ISO 13849-1) SIL 3 (safety integrity level according to IEC 61508)	
Probability of failure	Low demand mode: PFDavg in accordance with SIL 3 < 2.00E-05 High demand/continuous mode: PFH in accordance with SIL 3 < 1.00E-09 (altitude -1000 m to 3000 m) < 2.00E-09 (altitude >3000 m to 5000 m) For service life of 20 years and repair time of 100 hours	
Operating environment	Horizontal mounting -20 °C to 40 °C ¹ -20 °C to 60 °C ²	
	Vertical mounting -20 °C to 50 °C ²	Vertical mounting -20 °C to 40 °C ¹ -20 °C to 50 °C ²
	95% relative humidity at 25 °C during operation, without condensation, maximum	

¹ Operating temperature range using maximum voltages and maximum specifications

² Operating temperature range using rated voltages, 50% of maximum specifications, and alternate I/O active

Table A-35 CPU features

Technical data	Description	
User memory	Work Memory	300 Kbytes (Program) 750 Kbytes (Data)
	Load Memory	8 Mbytes (Internal) 32 Gbytes (using SD card)
	Retentive Memory	20 Kbytes
Onboard digital I/O	14 inputs / 10 outputs	
Process image size	1024 bytes of inputs (I) / 1024 bytes of outputs (Q)	
Bit memory size	8192 bytes (M)	
Temporary (local) memory	Per priority class, max.	64 Kbytes
	Per block, max.	16 Kbytes
Communication module/processor expansion	3 max. (must connect to the right of the CPU or to the right of another CM/CP)	
Signal module expansion (SM plus CM)	10 max.	
Signal board or Communication board expansion	2 max.	
High-speed counters	Max. number of high-speed counters	8 (any CPU or SB digital input)
	Max. rate, CPU inputs Ia.0 to Ia.5	100 kHz (80 kHz in quadrature mode)
	Max. rate, CPU inputs Ia.6 to Ib.5	30 kHz (20 kHz in quadrature mode)
	Max. rate, SB inputs	See SB specifications
Pulse outputs ¹	Max. number of pulse outputs	8 (any CPU or SB digital output)

¹ For CPU models with relay outputs, you must install a signal board (SB) containing DC digital outputs to use the pulse outputs.

Technical data	Description	
Pulse outputs ¹	Max. rate, CPU outputs Qa.0 to Qa.3	100 kHz
	Max. rate, CPU outputs Qa.4 to Qb.1	20 kHz
	Max. rate, SB outputs	See SB specifications
Pulse catch inputs	Yes, each onboard CPU digital input and SB digital input	
Time delay interrupts	20 total with 1 ms resolution	
Cyclic interrupts	20 total with 1 µs resolution	
Edge interrupts	Rising and falling for each onboard CPU digital input and SB digital input	
Memory card (Page 500)	SIMATIC memory card (optional).	
Motion control	Available Resources	800
	Required Resources	40 per speed-controlled axis
		80 per positioning axis
		160 per synchronous axis
		80 per external encoder
		20 per output cam
		160 per cam track
		40 per measuring input
	Available Extended Resources	40
PID	PID Compact	Yes, universal PID controller with integrated optimization
	PID 3Step	Yes, PID controller with integrated optimization for valves
	PID Temp	Yes, PID controller with integrated optimization for temperature
Real-time clock	Accuracy	+/- 60 seconds per month
	Retention time, super capacitor	20 days typical at 40 °C, 12 days minimum at 40 °C

¹ For CPU models with relay outputs, you must install a signal board (SB) containing DC digital outputs to use the pulse outputs.

A.6.2 Performance

Table A-36 Performance

Type of instruction ¹	Direct addressing (I, Q, and M)	DB accesses
Boolean	0.037 µs/instruction	
Move_Bool	0.067 µs/instruction	0.066 µs/instruction
Move_Word	0.027 µs/instruction	0.030 µs/instruction
Move_Real	0.027 µs/instruction	0.030 µs/instruction
Add_Real	0.119 µs/instruction	0.074 µs/instruction

¹ Many variables affect measured times. The above performance times are for the fastest instructions in each category and error-free programs.

A.6.3 Blocks, timers, and counters

Table A-37 Blocks, times, and counters

Element	Description	
Blocks	Type	OB, FB, FC, DB
	Max. number of elements	4000; Blocks (OB, FB, FC, DB) and UDTs
	Max. OB, FB, FC size	64 Kbytes
	Max. DB size (Optimized)	750 Kbytes Work Memory 16 Mbytes Load Memory
	Max. DB size (Non-optimized)	64 Kbytes (DBs with absolute addressing)
	Address range for FBs and FCs	1 to 65535
	Address range for DBs	1 to 59999
	Nesting depth per priority class ¹	24 (OB plus 23 more levels)
	Monitoring	Status of 8 code blocks can be monitored simultaneously.
Number of OBs per event class	Program cycle	100
	Startup	100
	Time delay interrupt	20 (one per event)
	Cyclic interrupt	20 (one per event)
	Hardware interrupt	50
	Time error interrupt	1
	Diagnostic error interrupt	1
	Pull or plug of modules	1
	Rack or station failure	1
	Time of day	20 (one per event)
	Synchronous Cycle	1
	Status	1
	Update	1
	Profile	1

¹ Safety programs use 2 nesting levels; the user program, therefore, has a nesting depth of 22 in safety programs.

Element	Description	
Number of OBs per event class	MC-Interpolator	1
	MC-Servo	1
	MC-PreServo	1
	MC-PostServo	1
	MC-LookAhead	1
	MC-PreInterpolator	1
	Programming error	1
	I/O access error	1
Timers	Type	IEC
	Quantity	Limited only by memory size
	Storage	Structure in DB, size depends upon time type
	IEC_TIMER	16 bytes
	IEC_LTIMER	28 bytes
Counters	Type	IEC
	Quantity	Limited only by memory size
	Storage	Structure in DB, size depends upon count type
	IEC_SCOUNTER, IEC_USCOUNTER	3 bytes
	IEC_COUNTER, IEC_UCOUNTER	6 bytes
	IEC_DCOUNTER, IEC_UDCOUNTER	12 bytes
	IEC_LCOUNTER, IEC_ULCOUNTER	24 bytes
Runtime Meters	Quantity	16

¹ Safety programs use 2 nesting levels; the user program, therefore, has a nesting depth of 22 in safety programs.

A.6.4 Communications

Table A-38 Communications

Technical data	Description
Number of ports	2 with an integrated switch
Type	Ethernet (RJ-45 connector)
Connections	88 connections max. (integrated into CPU) 10 reserved for ES/HMI/web
Data rates	100 Mb/s
Isolation (Page 84) (external signal to logic)	Transformer isolated, 1500 V AC (type test) ¹
Cable type	CAT5e shielded
Interfaces	1 PROFINET
	0 PROFIBUS

¹ Ethernet port isolation limits hazards during short term network faults to hazardous voltages. It does not conform to safety requirements for routine AC line voltage isolation.

Technical data	Description	
PROFINET Protocols	PROFINET IO controller	Yes
	PROFINET IO device	Yes
	SIMATIC communication	Yes
	Open IE communication	Yes
	Web server	Yes
	Media redundancy	Yes
PROFINET IO controller services	PG/OP communication	Yes
	S7 routing	Yes (requires more than one communication interface)
	Isochronous mode	Yes
	Open IE communication	Yes
	IRT	Yes
	MRP	Yes
	MRPD	Yes – Requires an IRT sync domain
	PROFenergy	Yes (per user program)
	Prioritized startup	Yes (max. 16 PROFINET devices)
	Number of connectable I/O devices, max.	31 (30 if I-Device is used, 29 if shared I-Device is used)
	Number of submodules, max.	512
	Number of IO devices that you can connect for RT, max.	31 (30 if I-Device is used, 29 if shared I-Device is used)
	Number of in line IO devices that you can connect for RT, max.	31
	Number of IO devices that you can connect for IRT, max.	31 (30 if I-Device is used, 29 if shared I-Device is used)
	Number of IO devices that can be activated/deactivated simultaneously, max.	8
	The minimum update time depends on the communication component set for PROFINET IO, on the number of IO devices, and the quantity of configured user data.	RT Send clock: 1 ms to 512 ms IRT Send clock: 1 ms to 512 ms (1 ms resolution)
PROFINET I-Device	Number of connections, max.	2
PROFINET I-Device services	PG/OP communication	Yes
	S7 routing	No
	Isochronous mode	No
	Open IE communication	Yes
	IRT	Yes
	MRP	Yes
	PROFenergy	Yes (per user program)
	Shared device	Yes

¹ Ethernet port isolation limits hazards during short term network faults to hazardous voltages. It does not conform to safety requirements for routine AC line voltage isolation.

Technical data	Description	
PROFINET I-Device services	Number of IO controllers with shared device, max.	2
SIMATIC communication	S7 communication as server	Yes
	S7 communication as client	Yes
	User data per job, max.	See TIA Portal information system (S7 communication, user data size)
Open IE communication	TCP/IP	Yes, 64 Kbytes max. data length Several passive connections per port
	ISO-on-TCP (RFC1006)	Yes, 64 Kbytes max. data length
	UDP	Yes, 2048 bytes max. data length 1472 bytes max. for UDP broadcast
	DHCP	Yes
	SNMP	Yes
	DCP	Yes
	LLDP	Yes
Near Field Communication (NFC)	Yes, with the S7-1200 G2 NFC app	
S7 message functions	Number of login stations for message functions, max.	32
	Program alarms	Yes
	Number of configurable program messages, max.	5000
	Number of loadable program messages in RUN, max.	2500
	Number of simultaneously active program alarms	600 program alarms 100 alarms for system diagnostics 160 for motion technology objects
Test commissioning functions	Joint commission (Team Engineering)	Yes, parallel online access possible for up to 5 engineering systems
	Program status	Yes, up to 8 blocks simultaneously (in total across all ES clients)
	Single step	No
	Breakpoints	No
	SIMATIC Controller Profiling	Yes
Monitor/modify	Variables	Inputs/outputs, memory bits, DBs, distributed I/Os, timers, counters
	Number of monitor variables, max.	200 per job
	Number of modify variables, max.	200 per job
Force	Variables	Peripheral inputs/outputs
	Number of variables, max.	200
Trace	Number of configurable traces	4
	Variables captured per trace, max.	16

¹ Ethernet port isolation limits hazards during short term network faults to hazardous voltages. It does not conform to safety requirements for routine AC line voltage isolation.

A.6 CPU 1214FC

Technical data	Description	
Trace	Data captured per trace, max.	512 KB
Diagnostics buffer	Number of entries, max.	500
	Retentive	100

¹ Ethernet port isolation limits hazards during short term network faults to hazardous voltages. It does not conform to safety requirements for routine AC line voltage isolation.

A.6.5 Power supply and sensor power

Table A-39 Power supply

Technical data	CPU 1214FC DC/DC/RLY	CPU 1214FC DC/DC/DC
Rated voltage	24 V DC	
Voltage range	20.4 to 28.8 V DC	
Reverse voltage protection	Yes	
Input current (CPU only)	245 mA at 24 V DC	145 mA at 24 V DC
Input current (with all accessories)	1100 mA at 24 V DC	1000 mA at 24 V DC
Inrush current	12 A max. at 28.8 V DC	
I ² t	0.5 A ² s	
Isolation (input power to logic)	Not isolated	
Hold up time (loss of power)	10 ms at 24 V DC	
Internal fuse	3 A, 250 V, slow blow not user replaceable	

Table A-40 Sensor power

Technical data	CPU 1214FC DC/DC/RLY	CPU 1214FC DC/DC/DC
Rated voltage	24 V DC	
Voltage range	L+ minus 4 V DC min.	
Output current rating	400 mA max. (short-circuit protected)	
Ripple noise (<10 MHz)	Same as input line	
Isolation (CPU logic to sensor power)	Not isolated	
Cable length	500 m shielded	
Cable size	0.2 mm ² to 1.5 mm ² (AWG 24 to 16)	

A.6.6 Digital inputs and outputs

Table A-41 Digital inputs

Technical data	CPU 1214FC DC/DC/RLY	CPU 1214FC DC/DC/DC
Number of inputs	14, in 1 isolation group of 14 inputs	
Assignment	Ia.0 to Ia.5 (high-speed) Ia.6 to Ib.5 (standard)	
Type	Sink/Source (IEC Type 1 sink)	
Rated voltage	24 V DC at 6 mA, nominal (high-speed) 24 V DC at 4 mA, nominal (standard)	
Continuous permissible voltage	30 V DC, max. at 8 mA, max. (high-speed) 30 V DC, max. at 6 mA, max. (standard)	
Logic 1 signal	15 V DC min. at 2.5 mA	
Logic 0 signal	5 V DC max. or 0.5 mA	
Isolation (field side to logic)	707 V DC (type test)	
Filter times (selectable by channel)	μ s settings: 0.1, 0.2, 0.4, 0.8, 1.6, 3.2, 6.4, 10.0, 12.8, 20.0 ms settings: 0.05, 0.1, 0.2, 0.4, 0.8, 1.6, 3.2, 6.4, 10.0, 12.8, 20.0	
HSC clock input rates (Logic 1 level = 15 to 30 V DC)	Single phase: 100 kHz (Ia.0 to Ia.5) Single phase: 30 kHz (Ia.6 to Ib.5) Quadrature phase: 80 kHz (Ia.0 to Ia.5) Quadrature phase: 20 kHz (Ia.6 to Ib.5)	
Cable length	500 m shielded, 300 m unshielded, 50 m shielded for HSC inputs	
Cable size	0.2 mm ² to 1.5 mm ² (AWG 24 to 16)	

Table A-42 Digital outputs

Technical data	CPU 1214FC DC/DC/RLY	CPU 1214FC DC/DC/DC
Number of outputs	10, in 1 isolation group of 10 outputs	
Assignment	Qa.0 to Qb.1	Qa.0 to Qa.3 (high-speed) Qa.4 to Qb.1 (standard)
Type	Relay, dry contact	Solid state – MOSFET (sourcing)
Rated voltage	--	24 V DC
Voltage range	5 to 30 V DC or 5 to 250 V AC	20.4 to 28.8 V DC
Logic 1 signal at max. current	--	20 V DC min.
Logic 0 signal with 10 k Ω load	--	0.1 V DC max.
Current	2.0 A max.	0.5 A max.
Minimum load ¹	125 mW DC / 500 mW AC	--
Lamp load	30 W DC / 200 W AC	5 W
ON state resistance	0.2 Ω max. when new	0.6 Ω max.

¹ When using relays at minimum load, avoid ambient temperatures below 0 °C.

² For CPU models with relay outputs, you must install a signal board (SB) containing DC digital outputs to use the pulse outputs.

³ Depending on your pulse receiver and cable, an additional load resistor (at least 10% of rated current) can improve pulse signal quality and noise immunity.

A.6 CPU 1214FC

Technical data	CPU 1214FC DC/DC/RLY	CPU 1214FC DC/DC/DC
Leakage current per point	--	10 µA max.
Overload protection	No	
Isolation (field side to logic)	1500 V AC (type test)	707 V DC (type test)
Isolation (coil to logic)	None	--
Current per common	20 A max. (10 A max. per pin)	5 A max.
Inductive clamp voltage	--	L+ minus 40 V, 1 W dissipation
Switching delay (Qa.0 to Qa.3)	10 ms max.	1.0 µs max., OFF to ON 3.0 µs max., ON to OFF
Switching delay (Qa.4 to Qb.1)	10 ms max.	5 µs max., OFF to ON 20 µs max., ON to OFF
Maximum relay switching frequency	1 Hz	--
Pulse Train Output (PTO) rate	Not recommended ²	100 kHz max. (Qa.0 to Qa.3) 20 kHz max. (Qa.4 to Qb.1) 2 Hz min. ³
Lifetime mechanical (no load)	10000000 open/close cycles	--
Lifetime contacts at rated load	100000 open/close cycles	--
Behavior on RUN to STOP	Last value or substitute value (default value 0)	
Control of a digital input	Yes	
Parallel outputs for redundant load control	Yes (with same common)	
Parallel outputs for increased load	No	
Cable length	500 m shielded, 150 m unshielded	
Cable size	0.2 mm ² to 1.5 mm ² (AWG 24 to 16)	

¹ When using relays at minimum load, avoid ambient temperatures below 0 °C.

² For CPU models with relay outputs, you must install a signal board (SB) containing DC digital outputs to use the pulse outputs.

³ Depending on your pulse receiver and cable, an additional load resistor (at least 10% of rated current) can improve pulse signal quality and noise immunity.

A.6.7 Wiring diagrams

The wiring diagrams and pin connector locations are shown below:

CPU 1214FC DC/DC/RLY

The diagram illustrates the wiring for the CPU 1214FC DC/DC/RLY module. It includes three main components: X80 (DC power wiring terminal), X10 (DC input wiring terminal), and X11 (Relay output wiring terminal).

X80: DC power wiring terminal (Gray, No keying)

DC power	L+		M
Pin #	1	3	5
Pin #	2	4	6
Sensor power	GND	L+	M

X10: DC input wiring terminal (Gray, No keying)

Signal	DI a.0	DI a.1	DI a.2	DI a.3	DI a.4	DI a.5	DI a.6	DI a.7
Pin #	1	3	5	7	9	11	13	15
Pin #	2	4	6	8	10	12	14	16
Signal	DI b.0	DI b.1	DI b.2	DI b.3	DI b.4	DI b.5	1M	1M

X11: Relay output wiring terminal (Orange, Type-A keying)

Signal	1L	DQ a.0	DQ a.1	DQ a.2	DQ a.3	DQ a.4
Pin #	1	3	5	7	9	11
Pin #	2	4	6	8	10	12
Signal	1L	DQ a.5	DQ a.6	DQ a.7	DQ b.0	DQ b.1

X80: DC power wiring terminal (Gray, No keying)

DC power	L+		M
Pin #	1	3	5
Pin #	2	4	6
Sensor power	GND	L+	M

X10: DC input wiring terminal (Gray, No keying)

Signal	DI a.0	DI a.1	DI a.2	DI a.3	DI a.4	DI a.5	DI a.6	DI a.7
Pin #	1	3	5	7	9	11	13	15
Pin #	2	4	6	8	10	12	14	16
Signal	DI b.0	DI b.1	DI b.2	DI b.3	DI b.4	DI b.5	1M	1M

X11: Relay output wiring terminal (Orange, Type-A keying)

Signal	1L	DQ a.0	DQ a.1	DQ a.2	DQ a.3	DQ a.4
Pin #	1	3	5	7	9	11
Pin #	2	4	6	8	10	12
Signal	1L	DQ a.5	DQ a.6	DQ a.7	DQ b.0	DQ b.1

① For additional noise immunity, jumper the 24 V DC Power "M" to Chassis Ground on the connector.

② For sinking inputs, connect "-" to "M" (shown). For sourcing inputs, connect "+" to "M".

CPU 1214FC DC/DC/DC											
					X80: DC power wiring terminal (Gray, No keying)						
					DC power	L+		M			
					Pin #	1	3	5			
					Pin #	2	4	6			
					Sensor power	GND	L+	M			
					X10: DC input wiring terminal (Gray, No keying)						
Signal	DI a.0	DI a.1	DI a.2	DI a.3	DI a.4	DI a.5	DI a.6	DI a.7			
Pin #	1	3	5	7	9	11	13	15			
Pin #	2	4	6	8	10	12	14	16			

① For additional noise immunity, jumper the 24 V DC Power "M" to Chassis Ground on the connector.

② For sinking inputs, connect "-" to "M" (shown). For sourcing inputs, connect "+" to "M".

CPU 1214FC DC/DC/DC									
	Signal	DI b.0	DI b.1	DI b.2	DI b.3	DI b.4	DI b.5	1M	1M
	X11: DC output wiring terminal (Gray, No keying)								
	Signal	2M	DQ a.0	DQ a.1	DQ a.2	DQ a.3	DQ a.4		
	Pin #	1	3	5	7	9	11		
	Pin #	2	4	6	8	10	12		
	Signal	2L+	DQ a.5	DQ a.6	DQ a.7	DQ b.0	DQ b.1		

① For additional noise immunity, jumper the 24 V DC Power "M" to Chassis Ground on the connector.

② For sinking inputs, connect "-" to "M" (shown). For sourcing inputs, connect "+" to "M".

A.7 Digital signal modules (SMs)

A.7.1 SM 1221 DI 16x24VDC

Table A-43 General specifications

Technical data	SM 1221 DI 16x24VDC
Article number	6ES7221-1BH50-0XB0
Dimensions W x H x D	30 x 125 x 100 mm
Weight (product/shipping)	166 grams / 203 grams
Power dissipation	3.2 W
Current consumption (bus)	90 mA max. (5 V DC)
Current consumption (24 V DC)	4.1 mA / input used

¹ Operating temperature range using maximum voltages and maximum specifications

Technical data	SM 1221 DI 16x24VDC
Operating environment	Horizontal mounting -20 °C to 60 °C ¹
	Vertical mounting -20 °C to 50 °C ¹
	95% relative humidity at 25 °C during operation, without condensation, maximum

¹ Operating temperature range using maximum voltages and maximum specifications

Table A-44 Digital inputs

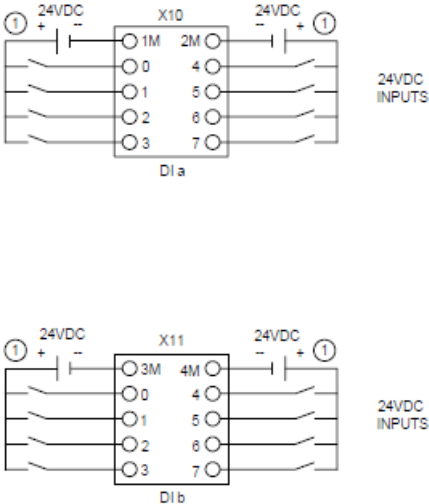
Technical data	SM 1221 DI 16x24VDC
Number of inputs	16, in 4 isolation groups of 4 inputs each
Type	Sink/Source (IEC Type 1 sink)
Rated voltage	24 V DC at 4.1 mA nominal
Continuous permissible voltage	30 V DC max.
Logic 1 signal	15 V DC min. at 2.5 mA
Logic 0 signal	5 V DC max. or 0.5 mA
Isolation (field side to logic)	707 V DC (type test)
Filter times (selectable in groups of 4)	0.2, 0.4, 0.8, 1.6, 3.2, 6.4, and 12.8 ms
Diagnostics	No
Cable length	500 m shielded, 300 m unshielded
Cable size	0.2 mm ² to 1.5 mm ² (AWG 24 to 16)

Wiring diagram

The wiring diagram and pin connector locations are shown below:

SM 1221 DI 16x24VDC				
	X10: Upper User Wiring Terminal (Gray, No Keying)			
	Signal	Pin #		Signal
	1M	1	2	2M
	DI a.0	3	4	DI a.4
	DI a.1	5	6	DI a.5
	DI a.2	7	8	DI a.6
	DI a.3	9	10	DI a.7
	X11: Lower User Wiring Terminal (Gray, No Keying)			
	Signal	Pin #		Signal
	3M	1	2	4M
	DI b.0	3	4	DI b.4
	DI b.1	5	6	DI b.5

① For sinking inputs, connect "-" to "M" (shown). For sourcing inputs, connect "+" to "M".

SM 1221 DI 16x24VDC					
	DI b.2	7	8	DI b.6	
	DI b.3	9	10	DI b.7	

① For sinking inputs, connect "-" to "M" (shown). For sourcing inputs, connect "+" to "M".

A.7.2 SM 1222 DQ 16x24VDC

Table A-45 General specifications

Technical data	SM 1222 DQ 16x24VDC
Article number	6ES7222-5BH50-0XB0
Dimensions W x H x D	30 x 125 x 100 mm
Weight (product/shipping)	173 grams / 210 grams
Power dissipation	3.5 W
Current consumption (bus)	120 mA max. (5 V DC)
Current consumption (24 V DC)	45 mA
Rated supply voltage	24 V DC
Supply voltage range	20.4 to 28.8 V DC
Reverse supply voltage protection	Yes

¹ Operating temperature range using maximum voltages and maximum specifications

Technical data	SM 1222 DQ 16x24VDC
Operating environment	Horizontal mounting -20 °C to 60 °C ¹
	Vertical mounting -20 °C to 50 °C ¹
	95% relative humidity at 25 °C during operation, without condensation, maximum

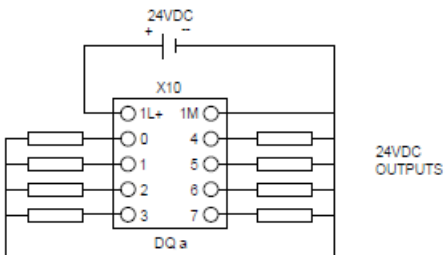
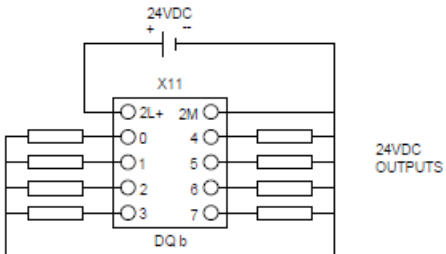
¹ Operating temperature range using maximum voltages and maximum specifications

Table A-46 Digital outputs

Technical data	SM 1222 DQ 16x24VDC
Number of outputs	16, in 2 isolation groups of 8 outputs each
Type	Solid state – MOSFET (sourcing)
Rated voltage	24 V DC
Voltage range	20.4 to 28.8 V DC
Logic 1 signal at max. current	L+ (-0.5 V)
Logic 0 signal with 10 kΩ load	0.1 V DC max.
Current	0.5 A max.
Lamp load	5 W
ON state resistance	0.6 Ω max.
Leakage current per point	10 µA max.
Overload protection	No
Isolation (field side to logic)	707 V DC (type test)
Current per common	4 A max.
Inductive clamp voltage	L+ minus 40 V, 1 W dissipation
Switching delay	50 µs max. OFF to ON 200 µs max. ON to OFF
Behavior on RUN to STOP	Last value or substitute value (default value 0)
Control of a digital input	Yes
Parallel outputs for redundant load control	Yes (with same common)
Parallel outputs for increased load	No
Diagnostics	24 V DC low voltage
Cable length	500 m shielded, 150 m unshielded
Cable size	0.2 mm ² to 1.5 mm ² (AWG 24 to 16)

Wiring diagram

The wiring diagram and pin connector locations are shown below:

SM 1222 DQ 16x24VDC			
	X10: Upper user wiring terminal (Gray, No keying)		
	Signal	Pin #	Signal
	1L+	1 2	1M
	DQ a.0	3 4	DQ a.4
	DQ a.1	5 6	DQ a.5
	DQ a.2	7 8	DQ a.6
	DQ a.3	9 10	DQ a.7
	X11: Lower user wiring terminal (Gray, No keying)		
	Signal	Pin #	Signal
	2L+	1 2	2M
	DQ b.0	3 4	DQ b.4
	DQ b.1	5 6	DQ b.5
	DQ b.2	7 8	DQ b.6
	DQ b.3	9 10	DQ b.7

A.7.3 SM 1222 DQ 16xRLY

Table A-47 General specifications

Technical data	SM 1222 DQ 16xRLY
Article number	6ES7222-5HH50-0XB0
Dimensions W x H x D	30 x 125 x 100 mm
Weight (product/shipping)	217 grams / 254 grams
Power dissipation	4.2 W
Current consumption (bus)	115 mA max. (5 V DC)
Current consumption (24 V DC)	10 mA plus 9 mA / relay coil used
Rated supply voltage	24 V DC
Supply voltage range	20.4 to 28.8 V DC
Reverse supply voltage protection	Yes

¹ Operating temperature range using maximum voltages and maximum specifications

² Operating temperature range using rated voltages, 50% of maximum specifications, and alternate I/O active

Technical data	SM 1222 DQ 16xRLY
Operating environment	Horizontal mounting -20 °C to 40 °C ¹ -20 °C to 60 °C ²
	Vertical mounting -20 °C to 40 °C ¹ -20 °C to 50 °C ²
	95% relative humidity at 25 °C during operation, without condensation, maximum

¹ Operating temperature range using maximum voltages and maximum specifications

² Operating temperature range using rated voltages, 50% of maximum specifications, and alternate I/O active

Table A-48 Digital outputs

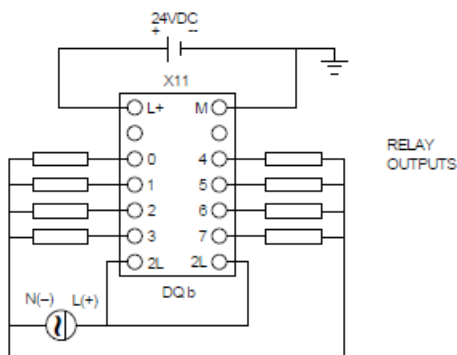
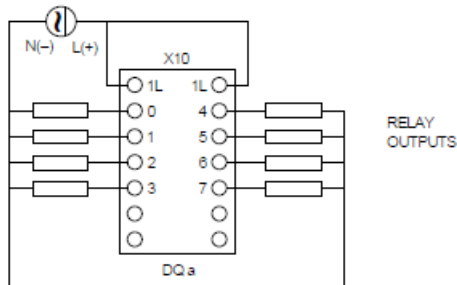
Technical data	SM 1222 DQ 16xRLY
Number of outputs	16, in 2 isolation groups of 8 outputs each
Type	Relay, mechanical
Voltage range	5 to 30 V DC or 5 to 250 V AC
Current	2.0 A max.
Minimum load ¹	125 mW DC / 500 mW AC
Lamp load	30 W DC / 200 W AC
ON state resistance	0.2 Ω max. when new
Overload protection	No
Isolation (field side to logic)	1500 V AC (type test)
Isolation (coil to logic)	None
Isolation between groups	1500 V AC
Current per common	16 A max. (10 A max. per pin)
Switching delay	10 ms max.
Maximum relay switching frequency	1 Hz
Lifetime mechanical (no load)	10000000 open/close cycles
Lifetime contacts at rated load (N.O. contact)	100000 open/close cycles
Behavior on RUN to STOP	Last value or substitute value (default value 0)
Control of a digital input	Yes
Parallel outputs for redundant load control	Yes (with same common)
Parallel outputs for increased load	No
Diagnostics	24 V DC low voltage
Cable length	500 m shielded, 150 m unshielded
Cable size	0.2 mm ² to 1.5 mm ² (AWG 24 to 16)

¹ When using relays at minimum load, avoid ambient temperatures below 0 °C.

Wiring diagram

The wiring diagram and pin connector locations are shown below:

SM 1222 DQ 16xRLY



X10: Upper User Wiring Terminal (Orange, Type-A Keying)

Signal	Pin #	Signal
1L	1	2
DQ a.0	3	4
DQ a.1	5	6
DQ a.2	7	8
DQ a.3	9	10
	11	12
	13	14

X11: Lower User Wiring Terminal (Orange, Type-A Keying)

Signal	Pin #	Signal
L+	1	2
	3	4
DQ b.0	5	6
DQ b.1	7	8
DQ b.2	9	10
DQ b.3	11	12
2L	13	14

A.7.4 SM 1223 DI 8x24VDC / DQ 8x24VDC

Table A-49 General specifications

Technical data	SM 1223 DI 8x24VDC / DQ 8x24VDC
Article number	6ES7223-5BH50-0XB0
Dimensions W x H x D	30 x 125 x 100 mm
Weight (product/shipping)	170 grams / 207 grams
Power dissipation	4.0 W
Current consumption (bus)	110 mA max. (5 V DC)
Current consumption (24 V DC)	60 mA plus 4.1 mA / input used
Rated supply voltage	24 V DC
Supply voltage range	20.4 to 28.8 V DC
Reverse supply voltage protection	Yes

¹ Operating temperature range using maximum voltages and maximum specifications

Technical data	SM 1223 DI 8x24VDC / DQ 8x24VDC
Operating environment	Horizontal mounting -20 °C to 60 °C ¹
	Vertical mounting -20 °C to 50 °C ¹
	95% relative humidity at 25 °C during operation, without condensation, maximum

¹ Operating temperature range using maximum voltages and maximum specifications

Table A-50 Digital inputs

Technical data	SM 1223 DI 8x24VDC / DQ 8x24VDC
Number of inputs	8, in 2 isolation groups of 4 inputs each
Type	Sink/Source (IEC Type 1 sink)
Rated voltage	24 V DC at 4 mA nominal
Continuous permissible voltage	30 V DC max.
Logic 1 signal	15 V DC min. at 2.5 mA
Logic 0 signal	5 V DC max. or 0.5 mA
Isolation (field side to logic)	707 V DC (type test)
Filter times (selectable in groups of 4)	0.2, 0.4, 0.8, 1.6, 3.2, 6.4, and 12.8 ms
Cable length	500 m shielded, 300 m unshielded
Cable size	0.2 mm ² to 1.5 mm ² (AWG 24 to 16)

Table A-51 Digital outputs

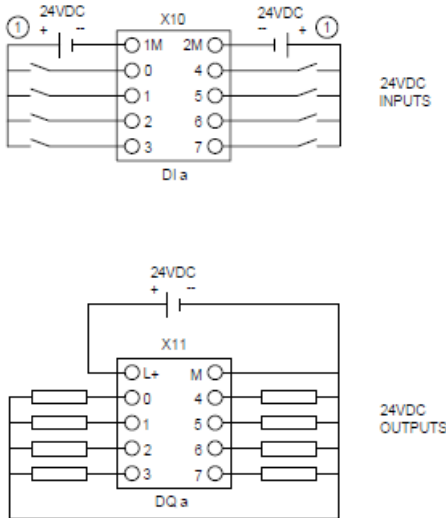
Technical data	SM 1223 DI 8x24VDC / DQ 8x24VDC
Number of outputs	8, in 1 isolation group of 8 outputs
Type	Solid state – MOSFET (sourcing)
Rated voltage	24 V DC
Voltage range	20.4 to 28.8 V DC
Logic 1 signal at max. current	L+ (-0.5 V)
Logic 0 signal with 10 kΩ load	0.1 V DC max.
Current	0.5 A max.
Lamp load	5 W
ON state resistance	0.6 Ω max.
Leakage current per point	10 µA max.
Overload protection	No
Isolation (field side to logic)	707 V DC (type test)
Current per common	4 A max.
Inductive clamp voltage	L+ minus 40 V, 1 W dissipation
Switching delay	50 µs max. OFF to ON 200 µs max. ON to OFF
Behavior on RUN to STOP	Last value or substitute value (default value 0)
Control of a digital input	Yes

A.7 Digital signal modules (SMs)

Technical data	SM 1223 DI 8x24VDC / DQ 8x24VDC
Parallel outputs for redundant load control	Yes (with same common)
Parallel outputs for increased load	No
Diagnostics	24 V DC low voltage
Cable length	500 m shielded, 150 m unshielded
Cable size	0.2 mm ² to 1.5 mm ² (AWG 24 to 16)

Wiring diagram

The wiring diagram and pin connector locations are shown below:

SM 1223 DI 8x24VDC / DQ 8x24VDC			
		X10: Upper User Wiring Terminal (Gray, No Keying)	
		Signal	Pin #
		1M	2M
		DI a.0	DI a.4
		DI a.1	DI a.5
		DI a.2	DI a.6
		DI a.3	DI a.7
		X11: Lower User Wiring Terminal (Gray, No Keying)	
		Signal	Pin #
		L+	M
		DQ a.0	DQ a.4
		DQ a.1	DQ a.5
		DQ a.2	DQ a.6
		DQ a.3	DQ a.7

① For sinking inputs, connect "-" to "M" (shown). For sourcing inputs, connect "+" to "M".

A.7.5 SM 1223 DI 8x24VDC / DQ 8xRLY

Table A-52 General specifications

Technical data	SM 1223 DI 8x24VDC / DQ 8xRLY
Article number	6ES7223-5PH50-0XB0
Dimensions W x H x D	30 x 125 x 100 mm
Weight (product/shipping)	194 grams / 231 grams
Power dissipation	4.8 W
Current consumption (bus)	105 mA max. (5 V DC)
Current consumption (24 V DC)	10 mA plus 4.1 mA / input used 9 mA / relay coil used
Rated supply voltage	24 V DC
Supply voltage range	20.4 to 28.8 V DC
Reverse supply voltage protection	Yes
Operating environment	Horizontal mounting -20 °C to 40 °C ¹ -20 °C to 60 °C ²
	Vertical mounting -20 °C to 40 °C ¹ -20 °C to 50 °C ²
	95% relative humidity at 25 °C during operation, without condensation, maximum

¹ Operating temperature range using maximum voltages and maximum specifications

² Operating temperature range using rated voltages, 50% of maximum specifications, and alternate I/O active

Table A-53 Digital inputs

Technical data	SM 1223 DI 8x24VDC / DQ 8xRLY
Number of inputs	8, in 2 isolation groups of 4 inputs each
Type	Sink/Source (IEC Type 1 sink)
Rated voltage	24 V DC at 4 mA nominal
Continuous permissible voltage	30 V DC max.
Logic 1 signal	15 V DC min. at 2.5 mA
Logic 0 signal	5 V DC max. or 0.5 mA
Isolation (field side to logic)	707 V DC (type test)
Filter times (selectable in groups of 4)	0.2, 0.4, 0.8, 1.6, 3.2, 6.4, and 12.8 ms
Cable length	500 m shielded, 300 m unshielded
Cable size	0.2 mm ² to 1.5 mm ² (AWG 24 to 16)

Table A-54 Digital outputs

Technical data	SM 1223 DI 8x24VDC / DQ 8xRLY
Number of outputs	8, in one isolation group of 8 outputs
Type	Relay, mechanical

¹ When using relays at minimum load, avoid ambient temperatures below 0 °C.

A.7 Digital signal modules (SMs)

Technical data	SM 1223 DI 8x24VDC / DQ 8xRLY
Voltage range	5 to 30 V DC or 5 to 250 V AC
Current	2.0 A max.
Minimum load ¹	125 mW DC / 500 mW AC
Lamp load	30 W DC / 200 W AC
ON state resistance	0.2 Ω max. when new
Overload protection	No
Isolation (field side to logic)	1500 V AC (type test)
Isolation (coil to logic)	None
Current per common	16 A max. (10 A. max per pin)
Switching delay	10 ms max.
Maximum relay switching frequency	1 Hz
Lifetime mechanical (no load)	10000000 open/close cycles
Lifetime contacts at rated load (N.O. contact)	100000 open/close cycles
Behavior on RUN to STOP	Last value or substitute value (default value 0)
Control of a digital input	Yes
Parallel outputs for redundant load control	Yes (with same common)
Parallel outputs for increased load	No
Diagnostics	24 V DC low voltage
Cable length	500 m shielded, 150 m unshielded
Cable size	0.2 mm ² to 1.5 mm ² (AWG 24 to 16)

¹ When using relays at minimum load, avoid ambient temperatures below 0 °C.

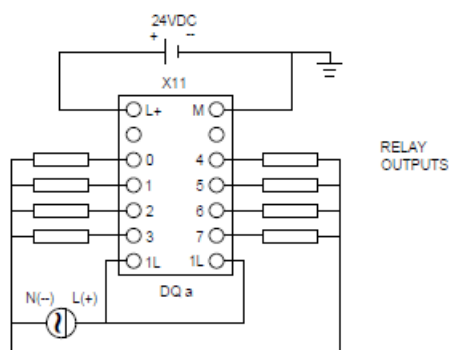
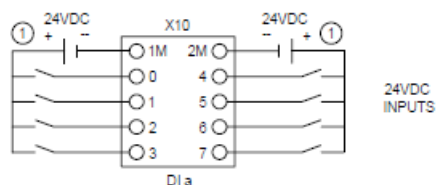
Wiring diagram

The wiring diagram and pin connector locations are shown below:

SM 1223 DI 8x24VDC / DQ 8xRLY				
	X10: Upper User Wiring Terminal (Gray, No Keying)			
	Signal	Pin #		Signal
	1M	1	2	2M
	DI a.0	3	4	DI a.4
	DI a.1	5	6	DI a.5
	DI a.2	7	8	DI a.6
	DI a.3	9	10	DI a.7
	X11: Lower User Wiring Terminal (Orange, Type-A Keying)			
	Signal	Pin #		Signal
	L+	1	2	M

① For sinking inputs, connect "-" to "M" (shown). For sourcing inputs, connect "+" to "M".

SM 1223 DI 8x24VDC / DQ 8xRLY



	3	4	
DQ a.0	5	6	DQ a.4
DQ a.1	7	8	DQ a.5
DQ a.2	9	10	DQ a.6
DQ a.3	11	12	DQ a.7
1L	13	14	1L

① For sinking inputs, connect "-" to "M" (shown). For sourcing inputs, connect "+" to "M".

A.7.6 SM 1223 DI 16x24VDC / DQ 16x24VDC

Table A-55 General specifications

Technical data	SM 1223 DI 16x24VDC / DQ 16x24VDC
Article number	6ES7223-5BL50-0XB0
Dimensions W x H x D	50 x 125 x 100 mm
Weight (product/shipping)	262 grams / 305 grams
Power dissipation	4.6 W
Current consumption (bus)	165 mA max. (5 V DC)
Current consumption (24 V DC)	45 mA plus 4.1 mA / input used
Operating environment	Horizontal mounting -20 °C to 60 °C ¹ Vertical mounting 20 °C to 50 °C ¹ 95% relative humidity at 25 °C during operation, without condensation, maximum

¹ Operating temperature range using maximum voltages and maximum specifications

A.7 Digital signal modules (SMs)

Table A-56 Digital inputs

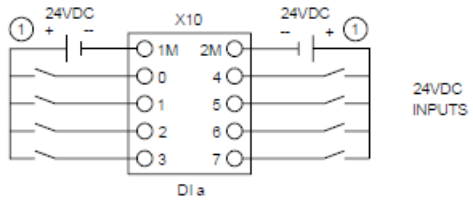
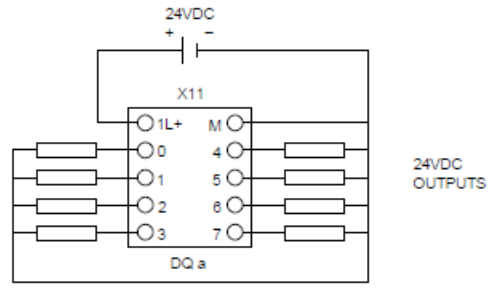
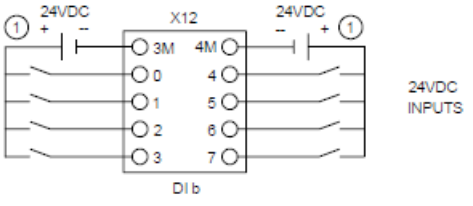
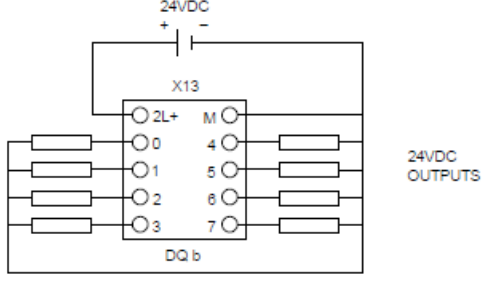
Technical data	SM 1223 DI 16x24VDC / DQ 16x24VDC
Number of inputs	16, in 4 isolation groups of 4 inputs each
Type	Sink/Source (IEC Type 1 sink)
Rated voltage	24 V DC at 4 mA nominal
Continuous permissible voltage	30 V DC max.
Logic 1 signal	15 V DC min. at 2.5 mA
Logic 0 signal	5 V DC max. or 0.5 mA
Isolation (field side to logic)	707 V DC (type test)
Filter times (selectable in groups of 4)	0.2, 0.4, 0.8, 1.6, 3.2, 6.4, and 12.8 ms
Cable length	500 m shielded, 300 m unshielded
Cable size	0.2 mm ² to 1.5 mm ² (AWG 24 to 16)

Table A-57 Digital outputs

Technical data	SM 1223 DI 16x24VDC / DQ 16x24VDC
Number of outputs	16, in 2 isolation groups of 8 outputs each
Type	Solid state – MOSFET (sourcing)
Rated voltage	24 V DC
Voltage range	20.4 to 28.8 V DC
Logic 1 signal at max. current	20 V DC min.
Logic 0 signal with 10 kΩ load	0.1 V DC max.
Current	0.5 A max.
Lamp load	5 W
ON state resistance	0.6 Ω max.
Leakage current per point	10 μA max.
Overload protection	No
Isolation (field side to logic)	707 V DC (type test)
Current per common	4 A max.
Inductive clamp voltage	L+ minus 40 V, 1 W dissipation
Switching delay	50 μs max. OFF to ON 200 μs max. ON to OFF
Behavior on RUN to STOP	Last value or substitute value (default value 0)
Control of a digital input	Yes
Parallel outputs for redundant load control	Yes (with same common)
Parallel outputs for increased load	No
Diagnostics	24 V DC low voltage
Cable length	500 m shielded, 150 m unshielded
Cable size	0.2 mm ² to 1.5 mm ² (AWG 24 to 16)

Wiring diagram

The wiring diagram and pin connector locations are shown below:

SM 1223 DI 16x24VDC / DQ 16x24VDC			
 24VDC INPUTS	X10: Upper Left User Wiring Terminal (Gray, No Keying)		
	Signal	Pin #	Signal
	1M	1 2	2M
	DI a.0	3 4	DI a.4
	DI a.1	5 6	DI a.5
	DI a.2	7 8	DI a.6
	DI a.3	9 10	DI a.7
 24VDC OUTPUTS	X11: Lower Left User Wiring Terminal (Gray, No Keying)		
	Signal	Pin #	Signal
	1L+	1 2	M
	DQ a.0	3 4	DQ a.4
	DQ a.1	5 6	DQ a.5
	DQ a.2	7 8	DQ a.6
	DQ a.3	9 10	DQ a.7
 24VDC INPUTS	X12: Upper Right User Wiring Terminal (Gray, No Keying)		
	Signal	Pin #	Signal
	3M	1 2	4M
	DI b.0	3 4	DI b.4
	DI b.1	5 6	DI b.5
	DI b.2	7 8	DI b.6
	DI b.3	9 10	DI b.7
 24VDC OUTPUTS	X13: Lower Right User Wiring Terminal (Gray, No Keying)		
	Signal	Pin #	Signal
	2L+	1 2	M
	DQ b.0	3 4	DQ b.4
	DQ b.1	5 6	DQ b.5
	DQ b.2	7 8	DQ b.6
	DQ b.3	9 10	DQ b.7

① For sinking inputs, connect "-" to "M" (shown). For sourcing inputs, connect "+" to "M".

A.7.7 SM 1223 DI 16x24VDC / DQ 16x24VDC Sink

Table A-58 General specifications

Technical data	SM 1223 DI 16x24VDC / DQ 16x24VDC Sink
Article number	6ES7223-5BL50-1XB0
Dimensions W x H x D	50 x 125 x 100 mm
Weight (product/shipping)	258 grams / 301 grams
Power dissipation	4.4 W
Current consumption (bus)	165 mA max. (5 V DC)
Current consumption (24 V DC)	40 mA plus 4.1 mA / input used
Operating environment	Horizontal mounting -20 °C to 60 °C ¹
	Vertical mounting -20 °C to 50 °C ¹
	95% relative humidity at 25 °C during operation, without condensation, maximum

¹ Operating temperature range using maximum voltages and maximum specifications

Table A-59 Digital inputs

Technical data	SM 1223 DI 16x24VDC / DQ 16x24VDC Sink
Number of inputs	16, in 4 isolation groups of 4 inputs each
Type	Sink/Source (IEC Type 1 sink)
Rated voltage	24 V DC at 4 mA nominal
Continuous permissible voltage	30 V DC max.
Logic 1 signal	15 V DC min. at 2.5 mA
Logic 0 signal	5 V DC max. or 0.5 mA
Isolation (field side to logic)	707 V DC (type test)
Filter times (selectable in groups of 4)	0.2, 0.4, 0.8, 1.6, 3.2, 6.4, and 12.8 ms
Cable length	500 m shielded, 300 m unshielded
Cable size	0.2 mm ² to 1.5 mm ² (AWG 24 to 16)

Table A-60 Digital outputs

Technical data	SM 1223 DI 16x24VDC / DQ 16x24VDC Sink
Number of outputs	16, in 2 isolation groups of 8 outputs each
Type	Solid state – MOSFET (sinking)
Rated voltage	24 V DC
Voltage range	20.4 to 28.8 V DC
Logic 1 signal at max. current	0.5 V DC
Logic 0 signal with 10 kΩ load	24 V (typical) minus 0.75 V DC
Current	0.5 A max.
Lamp load	5 W
ON state resistance	0.5 Ω max.

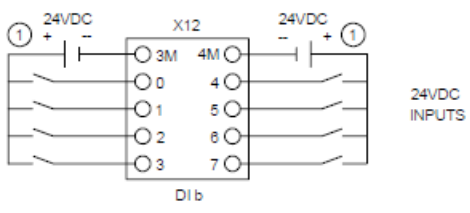
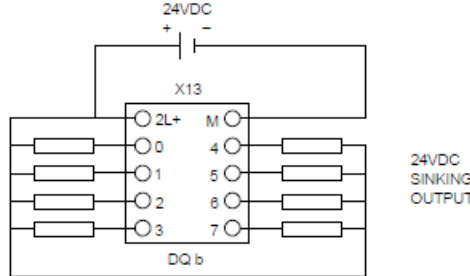
Technical data	SM 1223 DI 16x24VDC / DQ 16x24VDC Sink
Leakage current per point	75 µA max.
Overload protection	Yes, current limit protected range 1 A to 3.5 A
Isolation (field side to logic)	707 V DC (type test)
Current per common	4 A max.
Inductive clamp voltage	45 V
Switching delay	20 µs max. OFF to ON 350 µs max. ON to OFF
Behavior on RUN to STOP	Last value or substitute value (default value 0)
Control of a digital input	Yes (sourcing input)
Parallel outputs for redundant load control	Yes (with same common)
Parallel outputs for increased load	No
Diagnostics	24 V DC low voltage
Cable length	500 m shielded, 150 m unshielded
Cable size	0.2 mm ² to 1.5 mm ² (AWG 24 to 16)

Wiring diagram

The wiring diagram and pin connector locations are shown below:

SM 1223 DI 16x24VDC / DQ 16x24VDC Sink			
24VDC INPUTS	X10: Upper Left User Wiring Terminal (Gray, No Keying)		
	Signal	Pin #	Signal
	1M	1	2M
	DI a.0	3	DI a.4
	DI a.1	5	DI a.5
	DI a.2	7	DI a.6
24VDC SINKING OUTPUTS	X11: Lower Left User Wiring Terminal (Gray, No Keying)		
	Signal	Pin #	Signal
	1L+	1	M
	DQ a.0	3	DQ a.4
	DQ a.1	5	DQ a.5
	DQ a.2	7	DQ a.6
	X12: Upper Right User Wiring Terminal (Gray, No Keying)		
	Signal	Pin #	Signal
	3M	1	4M

① For sinking inputs, connect "-" to "M" (shown). For sourcing inputs, connect "+" to "M".

SM 1223 DI 16x24VDC / DQ 16x24VDC Sink				
	DI b.0	3	4	DI b.4
	DI b.1	5	6	DI b.5
	DI b.2	7	8	DI b.6
	DI b.3	9	10	DI b.7
	X13: Lower Right User Wiring Terminal (Gray, No Keying)			
	Signal	Pin #		Signal
	2L+	1	2	M
	DQ b.0	3	4	DQ b.4
	DQ b.1	5	6	DQ b.5
	DQ b.2	7	8	DQ b.6
	DQ b.3	9	10	DQ b.7

① For sinking inputs, connect "-" to "M" (shown). For sourcing inputs, connect "+" to "M".

A.7.8 SM 1223 DI 16x24VDC / DQ 16xRLY

Table A-61 General specifications

Technical data	SM 1223 DI 16x24VDC / DQ 16xRLY
Article number	6ES7223-5PL50-0XB0
Dimensions W x H x D	50 x 125 x 100 mm
Weight (product/shipping)	311 grams / 354 grams
Power dissipation	8.2 W
Current consumption (bus)	160 mA max. (5 V DC)
Current consumption (24 V DC)	175 mA plus 4.1 mA / input used plus 9.3 mA / relay coil used
Operating environment	Horizontal mounting -20 °C to 40 °C ¹ -20 °C to 60 °C ²
	Vertical mounting -20 °C to 40 °C ¹ -20 °C to 50 °C ²
	95% relative humidity at 25 °C during operation, without condensation, maximum

¹ Operating temperature range using maximum voltages and maximum specifications

² Operating temperature range using rated voltages, 50% of maximum specifications, and alternate I/O active

Table A-62 Digital inputs

Technical data	SM 1223 DI 16x24VDC / DQ 16xRLY
Number of inputs	16, in 4 isolation groups of 4 inputs each
Type	Sink/Source (IEC Type 1 sink)
Rated voltage	24 V DC at 4 mA nominal
Continuous permissible voltage	30 V DC max.
Logic 1 signal	15 V DC min. at 2.5 mA
Logic 0 signal	5 V DC max. or 0.5 mA
Isolation (field side to logic)	707 V DC (type test)
Filter times (selectable in groups of 4)	0.2, 0.4, 0.8, 1.6, 3.2, 6.4, and 12.8 ms
Cable length	500 m shielded, 300 m unshielded
Cable size	0.2 mm ² to 1.5 mm ² (AWG 24 to 16)

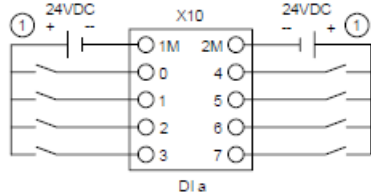
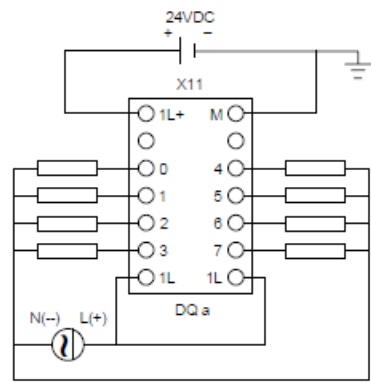
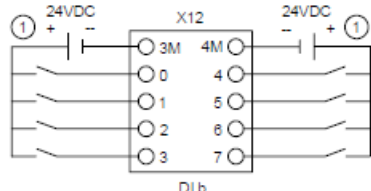
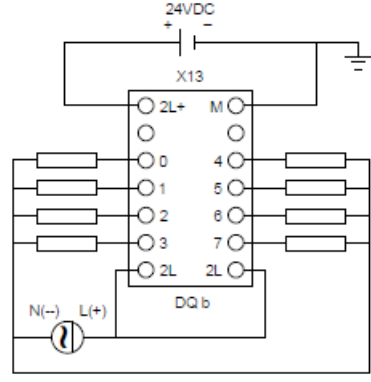
Table A-63 Digital outputs

Technical data	SM 1223 DI 16x24VDC / DQ 16xRLY
Number of outputs	16, in 2 isolation groups of 8 outputs each
Type	Relay, mechanical
Voltage range	5 to 30 V DC or 5 to 250 V AC
Current	2.0 A max.
Minimum load ¹	125 mW DC / 500 mW AC
Lamp load	30 W DC / 200 W AC
ON state resistance	0.2 Ω max. when new
Overload protection	No
Isolation (field side to logic)	1500 V AC (type test)
Isolation (coil to logic)	None
Current per common	16 A max. (10 A max. per pin)
Switching delay	10 ms max.
Maximum relay switching frequency	1 Hz
Lifetime mechanical (no load)	10,000,000 open/close cycles
Lifetime contacts at rated load (N.O. contact)	100,000 open/close cycles
Behavior on RUN to STOP	Last value or substitute value (default value 0)
Control of a digital input	Yes
Parallel outputs for redundant load control	Yes (with same common)
Parallel outputs for increased load	No
Diagnostics	24 V DC low voltage
Cable length	500 m shielded, 150 m unshielded
Cable size	0.2 mm ² to 1.5 mm ² (AWG 24 to 16)

Wiring diagram

The wiring diagram and pin connector locations are shown below:

SM 1223 DI 16x24VDC / DQ 16xRLY

 24VDC INPUTS	X10: Upper Left User Wiring Terminal (Gray, No Keying) <table><tr><th>Signal</th><th>Pin #</th><th>Signal</th></tr><tr><td>1M</td><td>1</td><td>2</td></tr><tr><td>DI a.0</td><td>3</td><td>4</td></tr><tr><td>DI a.1</td><td>5</td><td>6</td></tr><tr><td>DI a.2</td><td>7</td><td>8</td></tr><tr><td>DI a.3</td><td>9</td><td>10</td></tr></table>	Signal	Pin #	Signal	1M	1	2	DI a.0	3	4	DI a.1	5	6	DI a.2	7	8	DI a.3	9	10						
Signal	Pin #	Signal																							
1M	1	2																							
DI a.0	3	4																							
DI a.1	5	6																							
DI a.2	7	8																							
DI a.3	9	10																							
 RELAY OUTPUTS	X11: Lower Left User Wiring Terminal (Orange, Type-A Keying) <table><tr><th>Signal</th><th>Pin #</th><th>Signal</th></tr><tr><td>1L+</td><td>1</td><td>2</td></tr><tr><td></td><td>3</td><td>4</td></tr><tr><td>DQ a.0</td><td>5</td><td>6</td></tr><tr><td>DQ a.1</td><td>7</td><td>8</td></tr><tr><td>DQ a.2</td><td>9</td><td>10</td></tr><tr><td>DQ a.3</td><td>11</td><td>12</td></tr><tr><td>1L</td><td>13</td><td>14</td></tr></table>	Signal	Pin #	Signal	1L+	1	2		3	4	DQ a.0	5	6	DQ a.1	7	8	DQ a.2	9	10	DQ a.3	11	12	1L	13	14
Signal	Pin #	Signal																							
1L+	1	2																							
	3	4																							
DQ a.0	5	6																							
DQ a.1	7	8																							
DQ a.2	9	10																							
DQ a.3	11	12																							
1L	13	14																							
 24VDC INPUTS	X12: Upper Right User Wiring Terminal (Gray, No Keying) <table><tr><th>Signal</th><th>Pin #</th><th>Signal</th></tr><tr><td>3M</td><td>1</td><td>2</td></tr><tr><td>DI b.0</td><td>3</td><td>4</td></tr><tr><td>DI b.1</td><td>5</td><td>6</td></tr><tr><td>DI b.2</td><td>7</td><td>8</td></tr><tr><td>DI b.3</td><td>9</td><td>10</td></tr></table>	Signal	Pin #	Signal	3M	1	2	DI b.0	3	4	DI b.1	5	6	DI b.2	7	8	DI b.3	9	10						
Signal	Pin #	Signal																							
3M	1	2																							
DI b.0	3	4																							
DI b.1	5	6																							
DI b.2	7	8																							
DI b.3	9	10																							
 RELAY OUTPUTS	X13: Lower Right User Wiring Terminal (Orange, Type-A Keying) <table><tr><th>Signal</th><th>Pin #</th><th>Signal</th></tr><tr><td>2L+</td><td>1</td><td>2</td></tr><tr><td></td><td>3</td><td>4</td></tr><tr><td>DQ b.0</td><td>5</td><td>6</td></tr><tr><td>DQ b.1</td><td>7</td><td>8</td></tr><tr><td>DQ b.2</td><td>9</td><td>10</td></tr><tr><td>DQ b.3</td><td>11</td><td>12</td></tr><tr><td>2L</td><td>13</td><td>14</td></tr></table>	Signal	Pin #	Signal	2L+	1	2		3	4	DQ b.0	5	6	DQ b.1	7	8	DQ b.2	9	10	DQ b.3	11	12	2L	13	14
Signal	Pin #	Signal																							
2L+	1	2																							
	3	4																							
DQ b.0	5	6																							
DQ b.1	7	8																							
DQ b.2	9	10																							
DQ b.3	11	12																							
2L	13	14																							

① For sinking inputs, connect "-" to "M" (shown). For sourcing inputs, connect "+" to "M".

A.8 Analog signal modules (SMs)

A.8.1 SM 1231 AI 8x14bit

Table A-64 General specifications

Technical data	SM 1231 AI 8x14bit
Article number	6ES7231-4HF50-0XB0
Dimensions W x H x D	30 x 125 x 100 mm
Weight (product/shipping)	175 grams / 212 grams
Power dissipation	2.5 W
Current consumption (bus)	75 mA max. (5 V DC)
Current consumption (24 V DC)	45 mA
Rated supply voltage	24 V DC
Supply voltage range	20.4 to 28.8 V DC
Reverse supply voltage protection	Yes
Operating environment	Horizontal mounting -20 °C to 60 °C ¹
	Vertical mounting -20 °C to 50 °C ¹
	95% relative humidity at 25 °C during operation, without condensation, maximum

¹ Operating temperature range using maximum voltages and maximum specifications

Table A-65 Analog inputs

Technical data	SM 1231 AI 8x14bit	
Number of inputs	8	
Type	Voltage or current (differential), selectable in groups of 2	
Range	± 10 V, ± 5 V, ± 2.5 V, 0 to 20 mA or 4 to 20 mA	
Full scale range (data word)	-27648 to 27648 voltage / 0 to 27648 current	
Overshoot/undershoot range (data word)	Voltage: 32511 to 27649 / -27649 to -32512 Current: 32511 to 27649 / 0 to -4864	
Overflow/underflow (data word)	Voltage: 32767 to 32512 / -32513 to -32768 Current 0 to 20 mA: 32767 to 32512 / -4865 to -32768 Current 4 to 20 mA: 32767 to 32512 (values below -4864 indicate open wire)	
Resolution	13 bits plus sign bit	
Maximum withstand voltage/current	± 35 V / ± 40 mA	
Smoothing	None, weak, medium, or strong	
Noise rejection	400, 60, 50, or 10 Hz	
Input impedance	Before parameterization	≥ 1 M Ω
	Voltage	≥ 1 M Ω
	Current	< 290 Ω , > 270 Ω
Isolation	Field side to logic	None

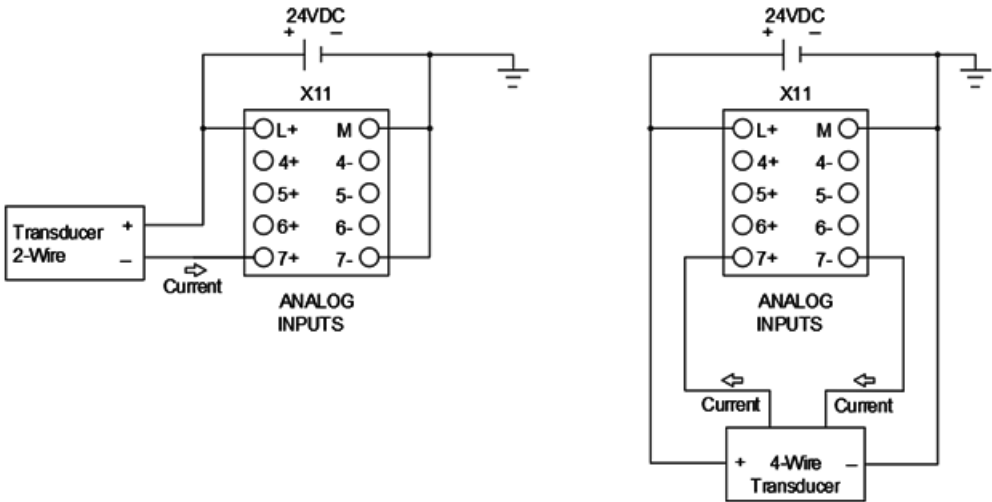
¹ Voltages outside the operational range applied to one channel can cause interference on other channels.

Technical data	SM 1231 AI 8x14bit	
Isolation	Logic to 24 V DC	None
	Field side to 24 V DC	None
	Channel to channel	None
Accuracy (25 °C / -20 to 60 °C)	$\pm 0.1\%$ / $\pm 0.2\%$ of full scale	
Measuring principle	Successive approximation	
Common mode rejection	40 dB, DC to 60 Hz	
Operational signal range ¹	Signal plus common mode voltage must be less than +12 V and greater than -12 V	
Diagnostics	Overflow/underflow	
	24 V DC low voltage	
	Open wire, 4 to 20 mA range only (if input is below -4864; 1.185 mA)	
Cable length	100 m, twisted and shielded	
Cable size	0.2 mm ² to 1.5 mm ² (AWG 24 to 16)	

¹ Voltages outside the operational range applied to one channel can cause interference on other channels.

Current measurement

You can implement current measurement with either a 2-wire transducer or a 4-wire transducer as shown below:



Wiring diagram

The wiring diagram and pin connector locations are shown below:

SM 1231 AI 8x14bit

X10: Upper User Wiring Terminal (Light Gray, Type-B Keying)

Signal	Pin #		Signal
AI 0+	1	2	AI 0-
AI 1+	3	4	AI 1-
AI 2+	5	6	AI 2-
AI 3+	7	8	AI 3-
	9	10	

X11: Lower User Wiring Terminal (Light Gray, Type-B Keying)

Signal	Pin #		Signal
L+	1	2	M
AI 4+	3	4	AI 4-
AI 5+	5	6	AI 5-
AI 6+	7	8	AI 6-
AI 7+	9	10	AI 7-

NOTE

When wiring and configuring analog input channels consider the following:

- Connect the positive input terminal to the negative input terminal on each unused voltage input channel.
- Set unused current input channels to the 0 to 20 mA range and/or disable broken wire error reporting.

Inputs configured for current mode do not conduct loop current if the module is not powered and configured.

Current input channels are operable only when you supply external power to the transmitter.

A.8.2 SM 1232 AQ 8x14bit

Table A-66 General specifications

Technical data	SM 1232 AQ 8x14bit
Article number	6ES7232-4HF50-0XB0
Dimensions W x H x D	30 x 125 x 100 mm
Weight (product/shipping)	173 grams / 210 grams
Power dissipation	5.6 W
Current consumption (bus)	90 mA max. (5 V DC)
Current consumption (24 V DC)	45 mA
Rated supply voltage	24 V DC
Supply voltage range	20.4 to 28.8 V DC
Reverse supply voltage protection	Yes
Operating environment	Horizontal mounting -20 °C to 40 °C ¹ -20 °C to 60 °C ²
	Vertical mounting -20 °C to 40 °C ¹ -20 °C to 50 °C ²
	95% relative humidity at 25 °C during operation, without condensation, maximum

¹ Operating temperature range using maximum voltages and maximum specifications

² Operating temperature range using rated voltages, 50% of maximum specifications, and alternate I/O active

Table A-67 Analog outputs

Technical data	SM 1232 AQ 8x14bit	
Number of outputs	8	
Type	Voltage or current	
Range	±10 V, 0 to 20 mA, or 4 to 20 mA	
Resolution	Voltage: 14 bits Current: 13 bits	
Full scale range (data word)	Voltage: -27648 to 27648 Current: 0 to 27648	
Accuracy (25 °C / -20 to 60 °C)	±0.3% / ±0.6% of full scale	
Settling time (95% of new value)	Voltage: 300 µs (R), 750 µs (1 µF) Current: 600 µs (1 mH), 2 ms (10 mH)	
Load impedance	Voltage: >= 1000 Ω Current: <= 600 Ω	
Maximum output short circuit current	Voltage: <= 24 mA Current: <= 24 mA	
Behavior on RUN to STOP	Last value or substitute value (default value 0)	
Isolation	Field side to logic	None
	24 V to output	None

¹ Short circuit detection is only possible when the output voltage is less than -0.5 V or greater than +0.5 V.

² Wire break detection is only possible when the output current is greater than 1 mA.

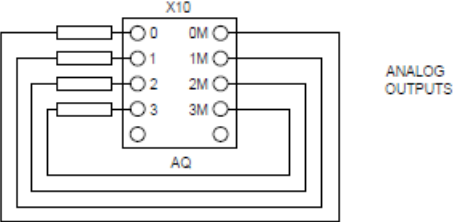
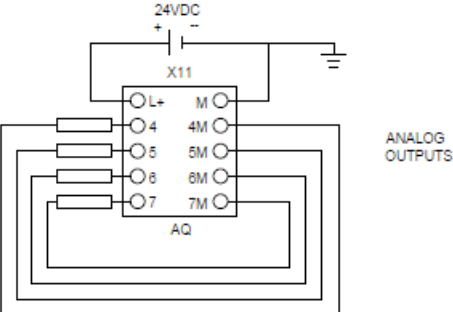
Technical data	SM 1232 AQ 8x14bit
Diagnostics	Overflow/underflow
	Short to ground (voltage mode only) ¹
	Wire break (current mode only) ²
	24 V DC low voltage
Cable length	100 m, twisted and shielded
Cable size	0.2 mm ² to 1.5 mm ² (AWG 24 to 16)

¹ Short circuit detection is only possible when the output voltage is less than -0.5 V or greater than +0.5 V.

² Wire break detection is only possible when the output current is greater than 1 mA.

Wiring diagram

The wiring diagram and pin connector locations are shown below:

SM 1232 AQ 8x14bit			
		X10: Upper User Wiring Terminal (Light Gray, Type-B Keying)	
		Signal	Pin #
		AQ 0	1
		AQ 1	3
		AQ 2	5
		AQ 3	7
			9
			10
		X11: Lower User Wiring Terminal (Light Gray, Type-B Keying)	
		Signal	Pin #
		L+	1
		AQ 4	3
		AQ 5	5
		AQ 6	7
		AQ 7	9
			10

A.8.3 SM 1233 AI 4x14bit / AQ 4x14bit

Table A-68 General specifications

Technical data	SM 1233 AI 4x14bit / AQ 4x14bit
Article number	6ES7233-4HF50-0XB0
Dimensions W x H x D	30 x 125 x 100 mm
Weight (product/shipping)	174 grams / 211 grams
Power dissipation	4.7 W
Current consumption (bus)	80 mA max. (5 V DC)
Current consumption (24 V DC)	40 mA
Rated supply voltage	24 V DC
Supply voltage range	20.4 to 28.8 V DC
Reverse supply voltage protection	Yes
Operating environment	Horizontal mounting -20 °C to 40 °C ¹ -20 °C to 60 °C ²
	Vertical mounting -20 °C to 40 °C ¹ -20 °C to 50 °C ²
	95% relative humidity at 25 °C during operation, without condensation, maximum

¹ Operating temperature range using maximum voltages and maximum specifications

² Operating temperature range using rated voltages, 50% of maximum specifications, and alternate I/O active

Table A-69 Analog inputs

Technical data	SM 1233 AI 4x14bit / AQ 4x14bit	
Number of inputs	4	
Type	Voltage or current (differential)	
Range	±10 V, ±5 V, ±2.5 V, 0 to 20 mA or 4 to 20 mA	
Full scale range (data word)	-27648 to 27648 voltage / 0 to 27648 current	
Overshoot/undershoot range (data word)	Voltage: 32511 to 27649 / -27649 to -32512 Current: 32511 to 27649 / 0 to -4864	
Overflow/underflow (data word)	Voltage: 32767 to 32512 / -32513 to -32768 Current 0 to 20 mA: 32767 to 32512 / -4865 to -32768 Current 4 to 20 mA: 32767 to 32512 (values below -4864 indicate open wire)	
Resolution	13 bits plus sign bit	
Maximum withstand voltage/current	±35 V / ±40 mA	
Smoothing	None, weak, medium, or strong	
Noise rejection	400, 60, 50, or 10 Hz	
Input impedance	Before parameterization	≥ 1 MΩ
	Voltage	≥ 1 MΩ
	Current	< 290 Ω, > 270 Ω
Isolation	Field side to logic	None

¹ Voltages outside the operational range applied to one channel can cause interference on other channels.

Technical data	SM 1233 AI 4x14bit / AQ 4x14bit	
Isolation	Logic to 24 V DC	None
	Field side to 24 V DC	None
	Channel to channel	None
Accuracy (25 °C / -20 to 60 °C)	±0.1% / ±0.2% of full scale	
Measuring principle	Successive approximation	
Common mode rejection	40 dB, DC to 60 Hz	
Operational signal range ¹	Signal plus common mode voltage must be less than +12 V and greater than -12 V	
Diagnostics	Overflow/underflow	
	24 V DC low voltage	
	Open wire, 4 to 20 mA range only (if input is below -4864; 1.185 mA)	
Cable length	100 m, twisted and shielded	
Cable size	0.2 mm ² to 1.5 mm ² (AWG 24 to 16)	

¹ Voltages outside the operational range applied to one channel can cause interference on other channels.

Table A-70 Analog outputs

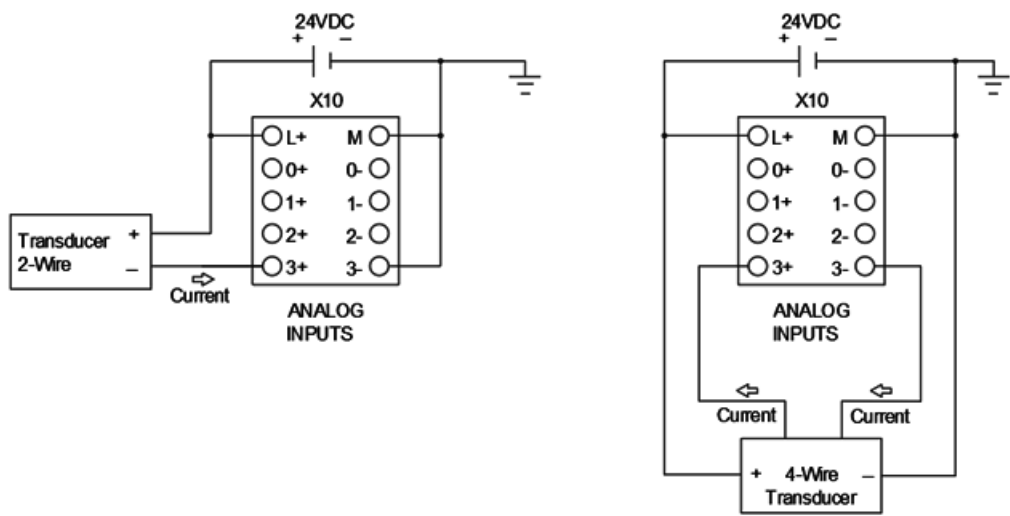
Technical data	SM 1233 AI 4x14bit / AQ 4x14bit	
Number of outputs	4	
Type	Voltage or current	
Range	± 10 V, 0 to 20 mA, or 4 to 20 mA	
Resolution	Voltage: 14 bits Current: 13 bits	
Full scale range (data word)	Voltage: -27648 to 27648 Current: 0 to 27648	
Accuracy (25 °C / -20 to 60 °C)	±0.3% / ±0.6% of full scale	
Settling time (95% of new value)	Voltage: 300 µs (R), 750 µs (1 µF) Current: 600 µs (1 mH), 2 ms (10 mH)	
Load impedance	Voltage: ≥ 1000 Ω Current: ≤ 600 Ω	
Maximum output short circuit current	Voltage: ≤ 24 mA Current: ≤ 24 mA	
Behavior on RUN to STOP	Last value or substitute value (default value 0)	
Isolation (field side to logic)	None	
Isolation (24 V to output)	None	
Diagnostics	Overflow/underflow	
	Short to ground (voltage mode only) ¹	
	Wire break (current mode only) ²	
	24 V DC low voltage	
Cable length	100 m, twisted and shielded	
Cable size	0.2 mm ² to 1.5 mm ² (AWG 24 to 16)	

¹ Short circuit detection is only possible when the output voltage is less than -0.5 V or greater than +0.5 V.

² Wire break detection is only possible when the output current is greater than 1 mA

Current measurement

You can implement current measurement with either a 2-wire transducer or a 4-wire transducer as shown below:

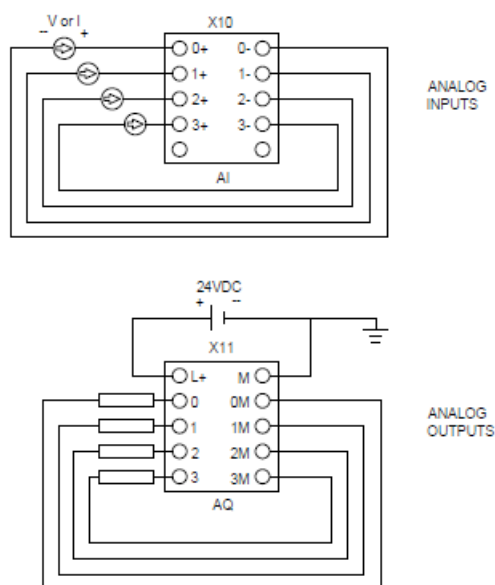


Wiring diagram

The wiring diagram and pin connector locations are shown below:

SM 1233 AI 4x14bit / AQ 4x14bit				
X10: Upper User Wiring Terminal (Light Gray, Type-B Keying)				
Signal	Pin #		Signal	
AI 0+	1	2	AI 0-	
AI 1+	3	4	AI 1-	
AI 2+	5	6	AI 2-	
AI 3+	7	8	AI 3-	
	9	10		
X11: Lower User Wiring Terminal (Light Gray, Type-B Keying)				
Signal	Pin #		Signal	
L+	1	2	M	
AQ 0	3	4	0M	
AQ 1	5	6	1M	

SM 1233 AI 4x14bit / AQ 4x14bit



AQ 2	7	8	2M
AQ 3	9	10	3M

NOTE

When wiring and configuring analog input channels consider the following:

- Connect the positive input terminal to the negative input terminal on each unused voltage input channel.
- Set unused current input channels to the 0 to 20 mA range and/or disable broken wire error reporting.

Inputs configured for current mode do not conduct loop current if the module is not powered and configured.

Current input channels are operable only when you supply external power to the transmitter.

A.8.4 Step response of the analog inputs

Table A-71 Step response (ms), 0 to full scale measured at 95%

Smoothing selection (sample averaging)	Noise reduction/rejection frequency (Integration time selection)			
	400 Hz (2.5 ms)	60 Hz (16.6 ms)	50 Hz (20 ms)	10 Hz (100 ms)
None (1 cycle): No averaging	4 ms	18 ms	22 ms	100 ms
Weak (4 cycles): 4 samples	9 ms	52 ms	63 ms	320 ms
Medium (16 cycles): 16 samples	32 ms	203 ms	241 ms	1200 ms
Strong (32 cycles): 32 samples	61 ms	400 ms	483 ms	2410 ms

A.8.5 Sample time and update times for the analog inputs

Table A-72 Sample time and update times for the analog inputs, all channels

Rejection frequency (Integration time)	Sample and module update times for all channels			
	400 Hz (2.5 ms)	60 Hz (16.6 ms)	50 Hz (20 ms)	10 Hz (100 ms)
4 channels	0.625 ms	4.17 ms	5 ms	25 ms
8 channels	1.25 ms	4.17 ms	5 ms	25 ms

A.8.6 Measurement ranges of the analog inputs for voltage and current

Table A-73 Analog input representation for voltage

System		Voltage measuring range				
Decimal	Hexadecimal	+/- 10 V	+/- 5 V	+/- 2.5 V	+/- 1.25 V	
32767	7FFF ¹	11.851 V	5.926 V	2.963 V	1.481 V	Overflow
32512	7F00					
32511	7EFF	11.759 V	5.879 V	2.940 V	1.470 V	Overshoot range
27649	6C01					
27648	6C00	10 V	5 V	2.5 V	1.250 V	Rated range
20736	5100	7.5 V	3.75 V	1.875 V	0.938 V	
1	1	361.7 μ V	180.8 μ V	90.4 μ V	45.2 μ V	
0	0	0 V	0 V	0 V	0 V	
-1	FFFF					
-20736	AF00	-7.5 V	-3.75 V	-1.875 V	-0.938 V	
-27648	9400	-10 V	-5 V	-2.5 V	-1.250 V	
-27649	93FF					Under-

¹ The channel can return 7FFF for one of the following reasons: overflow (as noted in this table), before valid values are available (for example, immediately upon a power up), or if a wire break is detected.

System		Voltage measuring range				
Decimal	Hexadecimal	+/- 10 V	+/- 5 V	+/- 2.5 V	+/- 1.25 V	
-32512	8100	-11.759 V	-5.879 V	-2.940 V	-1.470 V	shoot range
-32513	80FF					Underflow
-32768	8000	-11.851 V	-5.926 V	-2.963 V	-1.481 V	

¹ The channel can return 7FFF for one of the following reasons: overflow (as noted in this table), before valid values are available (for example, immediately upon a power up), or if a wire break is detected.

Table A-74 Analog input representation for current

System		Current measuring range		
Decimal	Hexadecimal	0 mA to 20 mA	4 mA to 20 mA	
32767	7FFF	> 23.52 mA	> 22.81 mA	Overflow
32511	7EFF	23.52 mA	22.81 mA	Overshoot range
27649	6C01			
27648	6C00	20 mA	20 mA	Nominal range
20736	5100	15 mA	16 mA	
1	1	723.4 nA	4 mA + 578.7 nA	
0	0	0 mA	4 mA	
-1	FFFF			Undershoot range
-4864	ED00	-3.52 mA	1.185 mA	
32767 ¹	7FFF		< 1.185 mA	Wire break (4 to 20 mA)
-32768	8000	< -3.52 mA		Underflow (0 to 20 mA)

¹ The wire break value of 32767 (16#7FFF) is always returned regardless of the state of the wire break alarm.

See also

[Determining the type of error from an analog module \(Page 352\)](#)

A.8.7 Measurement ranges of the analog outputs for voltage and current

Table A-75 Analog output representation for voltage

System		Voltage output range	
Decimal	Hexadecimal	+/- 10 V	
32767	7FFF	See note 1	Overflow
32512	7F00	See note 1	
32511	7EFF	11.76 V	Overshoot range
27649	6C01		
27648	6C00	10 V	Rated range
20736	5100	7.5 V	
1	0001	361.7 μ V	
0	0000	0 V	
-1	FFFF	-361.7 μ V	

¹ In an overflow or underflow condition, analog outputs take on the substitute value of the STOP mode.

System		Voltage output range	
Decimal	Hexadecimal	+/- 10 V	
-20736	AF00	-7.5 V	Rated range
-27648	9400	-10 V	
-27649	93FF		Undershoot range
-32512	8100	-11.76 V	
-32513	80FF	See note 1	Underflow
-32768	8000	See note 1	

¹ In an overflow or underflow condition, analog outputs take on the substitute value of the STOP mode.

Table A-76 Analog output representation for current

System		Current output range		
Decimal	Hexadecimal	0 mA to 20 mA	4 mA to 20 mA	
32767	7FFF	See note 1	See note 1	Overflow
32512	7F00	See note 1	See note 1	
32511	7EFF	23.52 mA	22.81 mA	Overshoot range
27649	6C01			
27648	6C00	20 mA	20 mA	Rated range
20736	5100	15 mA	16 mA	
1	1	723.4 nA	4 mA + 578.7 nA	
0	0	0 mA	4 mA	
-1	FFFF		4 mA to 578.7 nA	Undershoot range
-6912	E500		0 mA	
-6913	E4FF			Not possible. Output value limited to 0 mA.
-32512	8100			
-32513	80FF	See note 1	See note 1	Underflow
-32768	8000	See note 1	See note 1	

¹ In an overflow or underflow condition, analog outputs take on the substitute value of the STOP mode.

A.8.8 Basic operation of a thermocouple

A thermocouple is formed whenever two dissimilar metals are electrically bonded to each other. A voltage is generated across the bonded junction that is proportional to the junction temperature. This voltage is small; one microvolt could represent many degrees. Measuring the voltage from a thermocouple, compensating for extra junctions, and then linearizing the result forms the basis of temperature measurement using thermocouples.

The place where the two dissimilar wires are attached to each other forms the sensor thermocouple. The other ends of the thermocouple wires are each attached to a module or board at the signal connector.

Two more thermocouples are formed where the two wires are attached to the signal connector. The connector temperature causes a voltage that adds to the voltage from the sensor thermocouple. If this voltage is not corrected, then the temperature reported will deviate from the sensor temperature.

Cold junction compensation is used to compensate for the connector thermocouples. Thermocouple tables are based on a reference junction temperature, usually zero degrees Celsius. The cold junction compensation compensates the connector to zero degrees Celsius.

The cold junction compensation restores the voltage added by the connector thermocouples. The temperature of the module or board is measured internally, and then converted to a value to be added to the sensor conversion. The corrected sensor conversion is then linearized using the thermocouple tables.

For optimum operation of the cold junction compensation, the thermocouple module or board must be located in a thermally stable environment. Slow variation (less than 0.1 °C/minute) in ambient temperature is correctly compensated within the module or board specifications. Air movement across the module or board will also cause cold junction compensation errors.

If better cold junction error compensation is needed, an external iso-thermal terminal block can be used. The thermocouple board provides for use of a 0 °C referenced or 50 °C referenced terminal block.

A.8.9 SM 1231 AI 8xTC

Table A-77 General specifications

Technical data	SM 1231 AI 8xTC
Article number	6ES7231-5QF50-0XB0
Dimensions W x H x D	30 x 125 x 100 mm
Weight (product/shipping)	171 grams / 208 grams
Power dissipation	0.6 W
Current consumption (bus)	60 mA max. (5 V DC)
Current consumption (24 V DC)	15 mA
Rated supply voltage	24 V DC
Supply voltage range	20.4 to 28.8 V DC
Reverse supply voltage protection	Yes
Operating environment	Horizontal mounting -20 °C to 60 °C ¹
	Vertical mounting -20 °C to 50 °C ¹
	95% relative humidity at 25 °C during operation, without condensation, maximum

¹ Operating temperature range using maximum voltages and maximum specifications

Table A-78 Analog inputs

Technical data	SM 1231 AI 8xTC	
Number of inputs	8	
Sensor types	J, K, T, E, R & S, B, N, C, TXK/XK(L), voltage	
Ranges	See Selection tables for thermocouple sensors.	
Resolution Temperature	0.1 °C / 0.1 °F	
Resolution Voltage	15 bits plus sign	
Maximum withstand voltage	±35 V	
Noise rejection	85 dB for selected filter setting (10 Hz, 50 Hz, 60 Hz or 400 Hz)	
Common mode rejection	> 120 dB at 120 V AC	
Impedance	≥ 10 MΩ	
Isolation	Field side to logic	707 V DC (type test)
	Logic to 24 V DC	707 V DC (type test)
	Field side to 24 V DC	707 V DC (type test)
	Channel to channel	120 V AC
Accuracy	See Selection tables for thermocouple sensors.	
Repeatability	±0.05% of full scale	
Measuring principle	Integrating	
Module update time	See Noise reduction and update times for the Thermocouple module.	
Cold junction error	±1.5 °C	
Wire resistance	100 Ω max.	
Diagnostics	Overflow/underflow ¹	
	Wire break ^{2, 3}	
	24 V DC low voltage ¹	
Cable length	100 m to sensor max.	
Cable size	0.2 mm ² to 1.5 mm ² (AWG 24 to 16)	

¹ The overflow, underflow, and low voltage diagnostic alarm information is reported in the analog data values, even if the alarms are disabled in the module configuration.

² When wire break alarm is disabled and an open wire condition exists in the sensor wiring, the module can report random values.

³ The module performs wire break testing every 6 seconds, which extends the update time by 9 ms for each enabled channel once every 6 seconds.

The SM 1231 Thermocouple (TC) analog signal module measures the value of voltage connected to the module inputs. The temperature measurement type can be either "Thermocouple" or "Voltage".

- "Thermocouple": The value is reported in degrees multiplied by ten. (For example, 25.3 degrees is reported as decimal 253).
- "Voltage": The nominal range full scale value is decimal 27648.

Selection tables for thermocouple sensors

Table A-79 Thermocouple selection table

Type	Under-range minimum ¹	Nominal range low limit	Nominal range high limit	Over-range maximum ²	Normal range accuracy @ 25 °C ³	Normal range accuracy -20 °C to 60 °C ^{1, 2, 5}
J	-210.0 °C -346.0 °F	-150.0 °C -238.0 °F	1200.0 °C 2192.0 °F	1450.0 °C 2642.0 °F	±0.3 °C ±0.5 °F	±1.2 °C ±2.2 °F
K	-270.0 °C -454.0 °F	-200.0 °C -328.0 °F	1372.0 °C 2501.6 °F	1622.0 °C 2951.6 °F	±0.4 °C ±0.7 °F	±2.0 °C ±3.6 °F
T	-270.0 °C -454.0 °F	-200.0 °C -328.0 °F	400.0 °C 752.0 °F	540.0 °C 1004.0 °F	±0.5 °C ±0.9 °F	±1.0 °C ±1.8 °F
E	-270.0 °C -454.0 °F	-200.0 °C -328.0 °F	1000.0 °C 1832.0 °F	1200.0 °C 2192.0 °F	±0.3 °C ±0.5 °F	±0.6 °C ±1.1 °F
R & S	-50.0 °C -58.0 °F	100.0 °C 212.0 °F	1768.0 °C 3214.4 °F	2019.0 °C 3276.6 °F ⁴	±1.0 °C ±1.8 °F	±2.5 °C ±4.5 °F
B	0.0 °C 32.0 °F -- --	200.0 °C 392.0 °F 800.0 °C 1472.0 °F	800.0 °C 1472.0 °F 1820.0 °C 3276.6 °F ⁴	-- -- 1820.0 °C 3276.6 °F ⁴	±2.0 °C ±3.6 °F ±1.0 °C ±1.8 °F	±2.5 °C ±4.5 °F ±2.3 °C ±4.1 °F
N	-270.0 °C -454.0 °F	-200.0 °C -328.0 °F	1300.0 °C 2372.0 °F	1550.0 °C 2822.0 °F	±1.0 °C ±1.8 °F	±1.6 °C ±2.9 °F
C	0.0 °C 32.0 °F	100.0 °C 212.0 °F	2315.0 °C 3276.6 °F ⁴	2500.0 °C 3276.6 °F ⁴	±0.7 °C ±1.3 °F	±4.5 °C ±8.1 °F
TXK/XK(L)	-200.0 °C -328.0 °F	-150.0 °C 302.0 °F	800.0 °C 1472.0 °F	1050.0 °C 1922.0 °F	±0.6 °C ±1.1 °F	±1.2 °C ±2.2 °F
Voltage	-32512	-27648 -80mV	27648 80mV	32511	±0.05%	±0.1%

¹ Thermocouple values below the under-range minimum value are reported as -32768.

² Thermocouple values above the over-range maximum value are reported as 32767.

³ Internal cold junction error is ±1.5 °C for all ranges. This adds to the error values in this table. The module requires at least 30 minutes of warm-up time to meet this specification. For module ambient temperatures below -10 °C internal cold junction error can be greater than 1.5 °C.

⁴ Lower limit of 3276.6 °F with °F reporting

⁵ Cold junction compensation error has not been characterized for module ambient temperatures below 0 °C, and can exceed the specified value.

NOTE

Thermocouple channel

Each channel on the Thermocouple signal module can be configured with a different thermocouple type (selectable in the software during configuration of the module).

Table A-80 Noise reduction and update times for the Thermocouple module

Rejection frequency selection	Integration time	Module update time (seconds)
400 Hz (2.5 ms)	10 ms ¹	0.285
60 Hz (16.67 ms)	16.67 ms	0.445
50 Hz (20 ms)	20 ms	0.525
10 Hz (100 ms)	100 ms	2.450

¹ To maintain resolution and accuracy when the 400 Hz filter is selected, the integration time is 10 ms. This selection also rejects 100 Hz and 200 Hz noise.

Siemens recommends using a 100 ms integration time for measuring thermocouples. The use of smaller integration times increases the repeatability error of the temperature readings.

Internal calibration

After power is applied, the module performs internal calibration for the analog-to-digital converter. During this time the module reports a value of 32767 on each channel until the channel provides valid data. The STEP 7 program might need to allow for this initialization time. Because the initialization time varies based on the module's configuration, you must verify the behavior of the module in your system. If required, you can include logic in the STEP 7 program to accommodate the initialization time of the module.

You can implement this logic using a polling read in the "Startup OB" which blocks operation until the initialization is complete. You must implement the polling read with an immediate access. If the value of the thermocouple polling read is 32767, you must repeat the read until the value changes. For each module, use only the input channel with the greatest value for the thermocouple polling read. For example, if input channel number 2 is the highest used input channel, you should execute the thermocouple polling read on channel number 2. The module initializes the channels in order from 0 to 7.

Representation of analog values for Thermocouple Type J

A representation of the analog values of thermocouples type J is shown in the table below:

Table A-81 Representation of analog values of thermocouple type J

Type J in °C ¹	Units		Type J in °F ¹	Units		Range
	Decimal	Hexadecimal		Decimal	Hexadecimal	
> 1450.0	32767	7FFF	> 2642.0	32767	7FFF	Overflow
1450.0	14500	38A4	2642.0	26420	6734	Over-range
⋮	⋮	⋮	⋮	⋮	⋮	
1200.1	12001	2EE1	2192.2	21922	55A2	

¹ A value change of 1 indicates a temperature change of +/- one-tenth degree.

² Faulty wiring (for example, polarity reversal, or open inputs) or sensor error in the negative range (for example, wrong type of thermocouple) can cause the thermocouple module to signal underflow.

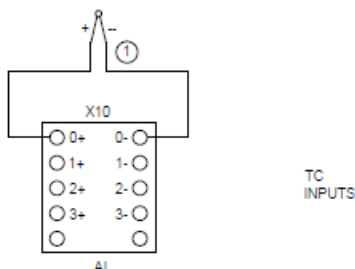
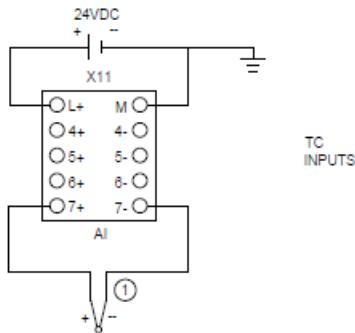
Type J in °C ¹	Units		Type J in °F ¹	Units		Range
	Decimal	Hexadecimal		Decimal	Hexadecimal	
1200.0 : -150	12000 : 1500	2EE0 : FA24	2192.0 : -238.0	21920 : -2380	55A0 : F6B4	Rated range
-150.1 : -210	-1501 : -2100	FA23 : F7CC	-238.1 : -346.0	-2381 : -3460	F6B3 : F27C	Under-range
< -210.0	-32768	8000	< -346.0	-32768	8000	Underflow ²

¹ A value change of 1 indicates a temperature change of +/- one-tenth degree.

² Faulty wiring (for example, polarity reversal, or open inputs) or sensor error in the negative range (for example, wrong type of thermocouple) can cause the thermocouple module to signal underflow.

Wiring diagram

The wiring diagram and pin connector locations are shown below:

SM 1231 AI 8xTC			
		X10: Upper user wiring terminal (Light gray, Type-B keying)	
		Signal	Pin #
		AI 0+	1
		AI 0-	2
		AI 1+	3
		AI 1-	4
		AI 2+	5
		AI 2-	6
		AI 3+	7
		AI 3-	8
			9
			10
		X11: Lower user wiring terminal (Light gray, Type-B keying)	
		Signal	Pin #
		L+	1
		M	2
		AI 4+	3
		AI 4-	4
		AI 5+	5
		AI 5-	6
		AI 6+	7
		AI 6-	8
		AI 7+	9
		AI 7-	10

① TC 1, 2, 3, 4, 5, and 6 are not shown for clarity.

NOTE

Connect the positive input terminal to the negative input terminal on each unused TC input channel. You can deactivate unused thermocouple channels. Deactivated channels do not report errors.

A.8.10 SM 1231 AI 4xRTD

Table A-82 General specifications

Technical data	SM 1231 AI 4xRTD
Article number	6ES7231-5PD50-0XB0
Dimensions W x H x D	30 x 125 x 100 mm
Weight (product/shipping)	169 g / 206 grams
Power dissipation	0.6 W
Current consumption (bus)	65 mA max. (5 V DC)
Current consumption (24 V DC)	15 mA
Rated supply voltage	24 V DC
Supply voltage range	20.4 to 28.8 V DC
Reverse supply voltage protection	Yes
Operating environment	Horizontal mounting -20 °C to 60 °C ¹
	Vertical mounting -20 °C to 50 °C ¹
	95% relative humidity at 25 °C during operation, without condensation, maximum

¹ Operating temperature range using maximum voltages and maximum specifications

Table A-83 Analog inputs

Technical data	SM 1231 AI 4xRTD	
Number of inputs	4	
Sensor types	See Selection table for the RTD sensors.	
Ranges	See Selection table for the RTD sensors.	
Resolution	Temperature	0.1 °C / 0.1 °F
	Resistance	15 bits plus sign
Maximum withstand voltage	± 35 V	
Noise rejection	85 dB for the selected noise reduction (10 Hz, 50 Hz, 60 Hz or 400 Hz)	
Common mode rejection	> 120 dB	

¹ The overflow, underflow and low voltage diagnostic alarm information is reported in the analog data values even if the alarms are disabled in the module configuration.

² For resistance ranges underflow detection is never enabled.

³ When wire break alarm is disabled and an open wire condition exists in the sensor wiring, the module can report random values.

⁴ Accuracy can be affected when the signal module is subjected to radio frequency radiation between 480 MHz to 800 MHz or when the signal module's ambient temperature changes at a rate of 3 °C per minute or faster.

Technical data	SM 1231 AI 4xRTD	
Impedance	>= 10 MΩ	
Isolation	Field side to logic	707 V DC (type test)
	Logic to 24 V DC	707 V DC (type test)
	Field side to 24 V DC	707 V DC (type test)
	Channel to channel	none
Accuracy	See Selection table for the RTD sensors. ⁴	
Repeatability	±0.05% of full scale	
Maximum sensor dissipation	0.2 mW	
Measuring principle	Integrating	
Module update time	See Noise reduction and update times for the RTD module.	
Diagnostics	Overflow/underflow ^{1, 2}	
	Wire break ³	
	24 V DC low voltage ¹	
Wire resistance	20 Ω, 2.7 Ω for 10 Ω RTD max.	
Cable length	100 m to sensor max.	
Cable size	0.2 mm ² to 1.5 mm ² (AWG 24 to 16)	

¹ The overflow, underflow and low voltage diagnostic alarm information is reported in the analog data values even if the alarms are disabled in the module configuration.

² For resistance ranges underflow detection is never enabled.

³ When wire break alarm is disabled and an open wire condition exists in the sensor wiring, the module can report random values.

⁴ Accuracy can be affected when the signal module is subjected to radio frequency radiation between 480 MHz to 800 MHz or when the signal module's ambient temperature changes at a rate of 3 °C per minute or faster.

The SM 1231 AI 4xRTD measures the value of resistance connected to the module inputs. The measurement type can be selected as either "Resistor" or "Thermal resistor".

- "Resistor": The nominal range full scale value is decimal 27648.
- "Thermal resistor": The value is reported in degrees multiplied by ten. (For example, 25.3 degrees is reported as decimal 253.) The climatic range values are reported in degrees multiplied by one hundred. (For example, 25.34 degrees is reported as decimal 2534.)

The SM 1231 AI 4xRTD uses a current to measure the resistance of the sensor. For resistance ranges and the RTD ranges of 200 ohms or less the current is 0.25 mA. For the 500- and 1000-ohm RTD ranges the current is 0.20 mA. This current is pulsed depending on the number of active channels on the module. For two active channels, the duty cycle for one channel is 50%. If four channels are active, the duty cycle for one channel is 25%. The maximum output voltage for an open circuit condition on the sensor is 3.3 V DC (measured between the I+ and I- terminals).

The SM 1231 AI 4xRTD supports measurements with 2-wire, 3-wire and 4-wire connections to the sensor resistor.

Selection table for the RTD sensors

Table A-84 Ranges and accuracy for the different sensors supported by the RTD module

Temperature coefficient	RTD type	Under range minimum ¹	Nominal range low limit	Nominal range high limit	Over range maximum ²	Normal range accuracy @ 25 °C	Normal range accuracy -20 °C to 60 °C
Pt 0.003850 ITS90 DIN EN 60751	Pt 100 climatic	-145.00 °C	-120.00 °C	145.00 °C	155.00 °C	±0.20 °C	±0.40 °C
	Pt 10	-243.0 °C	-200.0 °C	850.0 °C	1000.0 °C	±1.0 °C	±2.0 °C
	Pt 50	-243.0 °C	-200.0 °C	850.0 °C	1000.0 °C	±0.5 °C	±1.0 °C
	Pt 100						
	Pt 200						
	Pt 500						
	Pt 1000						
Pt 0.003902 Pt 0.003916 Pt 0.003920	Pt 100	-243.0 °C	-200.0 °C	850.0 °C	1000.0 °C	±0.5 °C	±1.0 °C
	Pt 200						
	Pt 500						
	Pt 1000						
Pt 0.003910	Pt 10	-273.2 °C	-240.0 °C	1100.0 °C	1295.0 °C	±1.0 °C	±2.0 °C
	Pt 50	-273.2 °C	-240.0 °C	1100.0 °C	1295.0 °C	±0.8 °C	±1.6 °C
	Pt 100						
	Pt 500						
Ni 0.006720 Ni 0.006180	Ni 100	-105.0 °C	-60.0 °C	250.0 °C	295.0 °C	±0.5 °C	±1.0 °C
	Ni 120						
	Ni 200						
	Ni 500						
	Ni 1000						
LG-Ni 0.005000	LG-Ni 1000	-105.0 °C	-60.0 °C	250.0 °C	295.0 °C	±0.5 °C	±1.0 °C
Ni 0.006170	Ni 100	-105.0 °C	-60.0 °C	180.0 °C	212.4 °C	±0.5 °C	±1.0 °C
Cu 0.004270	Cu 10	-240.0 °C	-200.0 °C	260.0 °C	312.0 °C	±1.0 °C	±2.0 °C
Cu 0.004260	Cu 10	-60.0 °C	-50.0 °C	200.0 °C	240.0 °C	±1.0 °C	±2.0 °C
	Cu 50	-60.0 °C	-50.0 °C	200.0 °C	240.0 °C	±0.6 °C	±1.2 °C
	Cu 100						
Cu 0.004280	Cu 10	-240.0 °C	-200.0 °C	200.0 °C	240.0 °C	±1.0 °C	±2.0 °C
	Cu 50	-240.0 °C	-200.0 °C	200.0 °C	240.0 °C	±0.7 °C	±1.4 °C
	Cu 100						

¹ RTD values below the under-range minimum value report -32768.

² RTD values above the over-range maximum value report +32767.

Table A-85 Resistance

Range	Under range minimum	Nominal range low limit	Nominal range high limit	Over range maximum ¹	Normal range accuracy @ 25 °C	Normal range accuracy -20 °C to 60 °C
150 Ω	n/a	0 (0 Ω)	27648 (150 Ω)	176.383 Ω	±0.05%	±0.1%
300 Ω	n/a	0 (0 Ω)	27648 (300 Ω)	352.767 Ω	±0.05%	±0.1%
600 Ω	n/a	0 (0 Ω)	27648 (600 Ω)	705.534 Ω	±0.05%	±0.1%

¹ Resistance values above the over-range maximum value are reported as +32767.

The module reports 32767 on any activated channel with no sensor connected. If open wire detection is also enabled, the module flashes the appropriate red LEDs.

When 500 Ω and 1000 Ω RTD ranges are used with other lower value resistors, the error can increase to two times the specified error.

Best accuracy is achieved for the 10 Ω RTD ranges if 4 wire connections are used.

The resistance of the connection wires in 2 wire mode causes an error in the sensor reading; therefore, accuracy is not guaranteed.

Table A-86 Noise reduction and update times for the RTD module

Rejection frequency selection	Integration time	Module update time (seconds)
400 Hz (2.5 ms)	10 ms ¹	4- / 2-wire: 0.142 3-wire: 0.285
60 Hz (16.67 ms)	16.67 ms	4- / 2-wire: 0.222 3-wire: 0.445
50 Hz (20 ms)	20 ms	4- / 2-wire: 0.262 3-wire: 0.505
10 Hz (100 ms)	100 ms	4- / 2-wire: 1.222 3-wire: 2.445

¹ To maintain resolution and accuracy when the 400 Hz filter is selected, the integration time is 10 ms. This selection also rejects 100 Hz and 200 Hz noise.

Internal calibration

After power is applied, the module performs internal calibration for the analog-to-digital converter. During this time the module reports a value of 32767 on each channel until the channel provides valid data. The STEP 7 program might need to allow for this initialization time. Because the initialization time varies based on the module's configuration, you must verify the behavior of the module in your system. If required, you can include logic in the STEP 7 program to accommodate the initialization time of the module.

You can implement this logic using a polling read in the "Startup OB" which blocks operation until the initialization is complete. You must implement the polling read with an immediate access. If the value of the RTD polling read is 32767, you must repeat the read until the value changes. For each module, use only the input channel with the greatest value for the RTD polling read. For example, if input channel number 2 is the highest used input channel, you should execute the RTD polling read on channel number 2. The module initializes the channels in order from 0 to 3.

Representation of analog values for RTDs

A representation of the digitized measured value for the RTD standard temperature range sensors is shown in the table below:

Table A-87 Representation of analog values for resistance temperature detectors PT 100, 200, 500, 1000 and PT 10, 50, 100, 500 GOST (0.003850) standard

Pt x00 standard in °C ¹	Units		Pt x00 standard in °F ¹	Units		Range
	Decimal	Hexadecimal		Decimal	Hexadecimal	
> 1000.0	32767	7FFF	> 1832.0	32767	7FFF	Overflow
1000.0	10000	2710	1832.0	18320	4790	Over-range
⋮	⋮	⋮	⋮	⋮	⋮	
850.1	8501	2135	1562.1	15621	3D05	
850.0	8500	2134	1562.0	15620	3D04	Rated range
⋮	⋮	⋮	⋮	⋮	⋮	
-200.0	-2000	F830	-328.0	-3280	F330	
-200.1	-2001	F82F	-328.1	-3281	F32F	Under-range
⋮	⋮	⋮	⋮	⋮	⋮	
-243.0	-2430	F682	-405.4	-4054	F02A	
< -243.0	-32768	8000	< -405.4	-32768	8000	Underflow

¹ A value change of 1 indicates a temperature change of +/- one-tenth degree.

Wiring diagram

The wiring diagram and pin connector locations are shown below:

SM 1231 AI 4xRTD				
	X10: Upper user wiring terminal (Light gray, Type-B keying)			
	Signal	Pin #		Signal
	AI I0+	1	2	AI I1+
	AI I0-	3	4	AI I1-
	AI M0+	5	6	AI M1+
	AI M0-	7	8	AI M1-
		9	10	
	X11: Lower user wiring terminal (Light gray, Type-B keying)			
	Signal	Pin #		Signal
	L+	1	2	M
	AI I2+	3	4	AI I3+
	AI I2-	5	6	AI I3-

- ① Loop-back unused RTD inputs
- ② 2-wire RTD connection represented
- ③ 3-wire RTD connection represented
- ④ 4-wire RTD connection represented

SM 1231 AI 4xRTD				
	AI M2+	7	8	AI M3+
	AI M2-	9	10	AI M3-

- ① Loop-back unused RTD inputs
- ② 2-wire RTD connection represented
- ③ 3-wire RTD connection represented
- ④ 4-wire RTD connection represented

NOTE

You can deactivate unused RTD channels. Deactivated channels do not report errors.
To avoid extra stabilization time, which is automatically added to an active unused channel, make the current loop continuous. For consistency, connect a resistor like the 2-wire RTD connection to the RTD module.

A.9 Digital signal boards (SBs)

A.9.1 SB 1221 DI 8x24VDC

Table A-88 General specifications

Technical data	SB 1221 DI 8x24VDC
Article number	6ES7221-3BF50-0XB0
Dimensions W x H x D	15 x 62 x 63 mm
Weight (product/shipping)	26 grams / 53 grams
Power dissipation	2.4 W
Current consumption (bus)	108 mA max. (5 V DC)
Current consumption (24 V DC)	6 mA / input used
Operating environment	Horizontal mounting -20 °C to 40 °C ¹ -20 °C to 60 °C ²
	Vertical mounting -20 °C to 40 °C ¹ -20 °C to 50 °C ²
	95% relative humidity at 25 °C during operation, without condensation, maximum

¹ Operating temperature range using maximum voltages and maximum specifications

² Operating temperature range using rated voltages, 50% of maximum specifications, and alternate I/O active

Table A-89 Digital inputs

Technical data	SB 1221 DI 8x24VDC
Number of inputs	8, in 1 isolation group of 8 inputs
Type	Sink/Source (IEC Type 1 sink)
Rated voltage	24 V DC at 5.8 mA nominal
Continuous permissible voltage	30 V DC max.
Logic 1 signal	15 V DC min. at 2.5 mA
Logic 0 signal	5 V DC max. or 0.5 mA
Isolation (field side to logic)	707 V DC (type test)
Filter times (selectable by channel)	µs settings: 0.1, 0.2, 0.4, 0.8, 1.6, 3.2, 6.4, 10.0, 12.8, 20.0 ms settings: 0.05, 0.1, 0.2, 0.4, 0.8, 1.6, 3.2, 6.4, 10.0, 12.8, 20.0
HSC clock input rates (Logic 1 Level = 15 to 30 V DC)	Single phase: 100 kHz max. Quadrature phase: 80 kHz max.
Cable length	500 m shielded, 300 m unshielded, 50 m shielded for HSC inputs
Cable size	0.2 mm ² to 0.8 mm ² (AWG 24 to 18)
Ferrule size	0.25 mm ² or 0.34 mm ² (AWG 24 or 22)

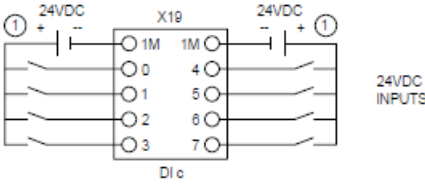
NOTE

When switching frequencies above 20 kHz, you must have a clean square wave. Consider the following options to improve the signal quality:

- Minimize the cable length.
- Change the driver from a sink or source only to a push-pull driver.
- Change to a higher quality cable.
- Reduce the circuit/components from 24 V to 5 V.
- Add an external load at the input.

Wiring diagram

The wiring diagram and pin connector locations are shown below:

SB 1221 DI 8x24VDC					
		X19: Upper User Wiring Terminal (Gray, No Keying)			
		Signal		Pin #	Signal
		1M	1	2	1M
		DI c.0	3	4	DI c.4
		DI c.1	5	6	DI c.5
		DI c.2	7	8	DI c.6
		DI c.3	9	10	DI c.7

① For sinking inputs, connect "-" to "M" (shown). For sourcing inputs, connect "+" to "M".

A.9.2 SB 1222 DQ 8x24VDC

Table A-90 General specifications

Technical data	SB 1222 DQ 8x24VDC
Article number	6ES7222-5BF50-0XB0
Dimensions W x H x D	15 x 62 x 63 mm
Weight (product/shipping)	29 grams / 53 grams
Power dissipation	1.0 W
Current consumption (bus)	30 mA max. (5 V DC)
Current consumption (24 V DC)	15 mA
Rated supply voltage	24 V DC
Supply voltage range	20.4 to 28.8 V DC
Reverse supply voltage protection	Yes
Operating environment	Horizontal mounting -20 °C to 40 °C ¹ -20 °C to 60 °C ²
	Vertical mounting -20 °C to 40 °C ¹ -20 °C to 50 °C ²
	95% relative humidity at 25 °C during operation, without condensation, maximum

¹ Operating temperature range using maximum voltages and maximum specifications

² Operating temperature range using rated voltages, 50% of maximum specifications, and alternate I/O active

Table A-91 Digital outputs

Technical data	SB 1222 DQ 8x24VDC
Number of outputs	8, in 1 isolation group of 8 outputs
Type	Push-pull
Rated voltage	24 V DC
Voltage range	20.4 to 28.8 V DC
Logic 1 signal at max. current	L+ minus 1.5 V
Logic 0 signal at max. current	1.0 V DC max.
Current	0.1 A max.
ON state resistance	6 Ω max.
OFF state resistance	10 Ω max.
Leakage current per point	10 µA max.
Pulse Train Output (PTO) rate	100 kHz max., 2 Hz min.
Overload protection	Yes
Isolation (field side to logic)	707 V DC (type test)
Current per common	0.8 A max.
Inductive clamp voltage	0 V, 1 W dissipation
Switching delay	1.5 µs + 300 ns rise 1.5 µs + 300 ns fall
Behavior on RUN to STOP	Last value or substitute value (default value 0)

Technical data	SB 1222 DQ 8x24VDC
Control of a digital input	Yes
Parallel outputs for redundant load control	Yes
Parallel outputs for increased load	No
Diagnostics	24 V DC low voltage
Cable length	500 m shielded, 150 m unshielded, 50 m shielded for PTO outputs
Cable size	0.2 mm ² to 0.8 mm ² (AWG 24 to 18)
Ferrule size	0.25 mm ² or 0.34 mm ² (AWG 24 or 22)

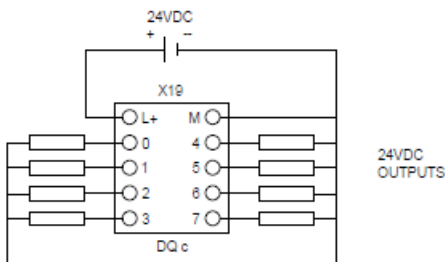
NOTE

When switching frequencies above 20 kHz, you must have a clean square wave. Consider the following options to improve the signal quality:

- Minimize the cable length.
 - Change the driver from a sink or source only to a push-pull driver.
 - Change to a higher quality cable.
 - Reduce the circuit/components from 24 V to 5 V.
 - Add an external load at the input.
-

Wiring diagram

The wiring diagram and pin connector locations are shown below:

SB 1222 DQ 8x24VDC			
	X19: Upper User Wiring Terminal (Gray, No Keying)		
	Signal	Pin #	Signal
	L+	1 2	M
	DQ c.0	3 4	DQ c.4
	DQ c.1	5 6	DQ c.5
	DQ c.2	7 8	DQ c.6
	DQ c.3	9 10	DQ c.7

⚠ WARNING

Risk of current leakage from ungrounded connections

Loss of the ground wire connection to the high-speed DQ SBs can allow enough leakage current to activate a DC load resulting in unexpected equipment operation.

Ensure that the M connection wire is securely grounded. If the outputs are used for critical DC load applications, exercise extra caution by using a redundant ground wire to the SB.

Unexpected equipment operation can result in property damage, severe personal injury, and death.

A.9.3 SB 1223 DI 4x24VDC / DQ 4x24VDC

Table A-92 General specifications

Technical data	SB 1223 DI 4x24VDC / DQ 4x24VDC
Article number	6ES7223-7BF50-0XB0
Dimensions W x H x D	15 x 62 x 63 mm
Weight (product/shipping)	28 grams / 55 grams
Power dissipation	1.7 W
Current consumption (bus)	48 mA max. (5 V DC)
Current consumption (24 V DC)	15 mA plus 6 mA / input used
Rated supply voltage	24 V DC
Supply voltage range	20.4 to 28.8 V DC
Reverse supply voltage protection	Yes

¹ Operating temperature range using maximum voltages and maximum specifications

² Operating temperature range using rated voltages, 50% of maximum specifications, and alternate I/O active

Technical data	SB 1223 DI 4x24VDC / DQ 4x24VDC
Operating environment	Horizontal mounting -20 °C to 40 °C ¹ -20 °C to 60 °C ²
	Vertical mounting -20 °C to 40 °C ¹ -20 °C to 50 °C ²
	95% relative humidity at 25 °C during operation, without condensation, maximum

¹ Operating temperature range using maximum voltages and maximum specifications

² Operating temperature range using rated voltages, 50% of maximum specifications, and alternate I/O active

Table A-93 Digital inputs

Technical data	SB 1223 DI 4x24VDC / DQ 4x24VDC
Number of inputs	4, in 1 isolation group of 4 inputs (no isolation inputs to outputs)
Type	Sink/Source (IEC Type 1 sink)
Rated voltage	24 V DC at 4 mA nominal
Continuous permissible voltage	30 V DC max.
Logic 1 signal	15 V DC min. at 2.5 mA
Logic 0 signal	5 V DC max. or 0.5 mA
Isolation (field side to logic)	707 V DC (type test)
Filter times (selectable by channel)	µs settings: 0.1, 0.2, 0.4, 0.8, 1.6, 3.2, 6.4, 10.0, 12.8, 20.0 ms settings: 0.05, 0.1, 0.2, 0.4, 0.8, 1.6, 3.2, 6.4, 10.0, 12.8, 20.0
HSC clock input rates (Logic 1 Level = 15 to 30 V DC)	Single phase: 100 kHz max. Quadrature phase: 80 kHz max.
Cable length	500 m shielded, 300 m unshielded, 50 m shielded for HSC inputs
Cable size	0.2 mm ² to 0.8 mm ² (AWG 24 to 18)
Ferrule size	0.25 mm ² or 0.34 mm ² (AWG 24 or 22)

Table A-94 Digital outputs

Technical data	SB 1223 DI 4x24VDC / DQ 4x24VDC
Number of outputs	4, in 1 isolation group of 4 outputs (no isolation outputs to inputs)
Type	Push-pull
Rated voltage	24 V DC
Voltage range	20.4 to 28.8 V DC
Logic 1 signal at max. current	L+ minus 1.5 V
Logic 0 signal at max. current	1.0 V DC max.
Current	0.1 A max.
ON state resistance	6 Ω max.
OFF state resistance	10 Ω max.
Leakage current per point	10 µA max.
Pulse Train Output (PTO) rate	100 kHz max., 2 Hz min.
Overload protection	Yes
Isolation (field side to logic)	707 V DC (type test)

Technical data	SB 1223 DI 4x24VDC / DQ 4x24VDC
Current per common	0.4 A max.
Inductive clamp voltage	0 V, 1 W dissipation
Switching delay	1.5 μ s + 300 ns rise 1.5 μ s + 300 ns fall
Behavior on RUN to STOP	Last value or substitute value (default value 0)
Control of a digital input	Yes
Parallel outputs for redundant load control	Yes
Parallel outputs for increased load	No
Diagnostics	24 V DC low voltage
Cable length	500 m shielded, 150 m unshielded, 50 m shielded for PTO outputs
Cable size	0.2 mm ² to 0.8 mm ² (AWG 24 to 18)
Ferrule size	0.25 mm ² or 0.34 mm ² (AWG 24 or 22)

NOTE

When switching frequencies above 20 kHz, you must have a clean square wave. Consider the following options to improve the signal quality:

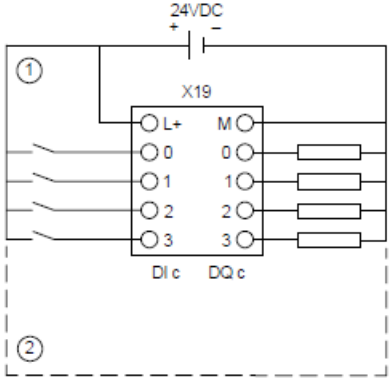
- Minimize the cable length.
- Change the driver from a sink or source only to a push-pull driver.
- Change to a higher quality cable.
- Reduce the circuit/components from 24 V to 5 V.
- Add an external load at the input.

Wiring diagram

The wiring diagram and pin connector locations are shown below:

SB 1223 DI 4x24VDC / DQ 4x24VDC				
		X19: Upper User Wiring Terminal (Gray, No Keying)		
		Signal	Pin #	Signal
		L+	1 2	M
		DI c.0	3 4	DQ c.0
		DI c.1	5 6	DQ c.1

- ① Wire the input common to (+) when configuring sinking inputs in TIA Portal (shown).
- ② Wire the input common to (-) when configuring sourcing inputs in TIA Portal.

SB 1223 DI 4x24VDC / DQ 4x24VDC				
	DI c.2	7	8	DQ c.2
	DI c.3	9	10	DQ c.3

- ① Wire the input common to (+) when configuring sinking inputs in TIA Portal (shown).
② Wire the input common to (-) when configuring sourcing inputs in TIA Portal.

⚠ WARNING

Risk of current leakage from ungrounded connections

Loss of the ground wire connection to the high-speed DQ SBs can allow enough leakage current to activate a DC load resulting in unexpected equipment operation.

Ensure that the M connection wire is securely grounded. If the outputs are used for critical DC load applications, exercise extra caution by using a redundant ground wire to the SB.

Unexpected equipment operation can result in property damage, severe personal injury, and death.

A.9.4 SB 1223 DI 4x5VDC / DQ 4x5VDC

Table A-95 General specifications

Technical data	SB 1223 DI 4x5VDC / DQ 4x5VDC
Article number	6ES7223-7AF50-0XB0
Dimensions W x H x D	15 x 62 x 63 mm
Weight (product/shipping)	28 grams / 55 grams
Power dissipation	1.0 W
Current consumption (bus)	60 mA max. (5 V DC)
Current consumption (5 V DC)	12 mA plus 15 mA per point used (source)
Rated supply voltage	5 V DC

¹ Operating temperature range using maximum voltages and maximum specifications

² Operating temperature range using rated voltages, 50% of maximum specifications, and alternate I/O active

Technical data	SB 1223 DI 4x5VDC / DQ 4x5VDC
Supply voltage range	4.25 to 6 V DC
Reverse supply voltage protection	Yes
Operating environment	Horizontal mounting -20 °C to 40 °C ¹ -20 °C to 60 °C ²
	Vertical mounting -20 °C to 40 °C ¹ -20 °C to 50 °C ²
	95% relative humidity at 25 °C during operation, without condensation, maximum

¹ Operating temperature range using maximum voltages and maximum specifications

² Operating temperature range using rated voltages, 50% of maximum specifications, and alternate I/O active

Table A-96 Digital inputs

Technical data	SB 1223 DI 4x5VDC / DQ 4x5VDC
Number of inputs	4, in 1 isolation group of 4 inputs (no isolation inputs to outputs)
Type	Source
Rated voltage	5 V DC at 15 mA nominal
Continuous permissible voltage	6 V DC max.
Logic 1 signal	0 V (20 mA) to L+ minus 2.0 V (5.1 mA) min.
Logic 0 signal	L+ minus 1.0 V (2.2 mA) to L+ (0 mA) max.
Isolation (field side to logic)	707 V DC (type test)
Filter times (selectable by channel)	µs settings: 0.1, 0.2, 0.4, 0.8, 1.6, 3.2, 6.4, 10.0, 12.8, 20.0 ms settings: 0.05, 0.1, 0.2, 0.4, 0.8, 1.6, 3.2, 6.4, 10.0, 12.8, 20.0
HSC clock input rates (Logic 1 Level = 2.5 to 6 V DC)	Single phase: 200 kHz max. Quadrature phase: 160 kHz max.
Cable length	50 m shielded twisted pair
Cable size	0.2 mm ² to 0.8 mm ² (AWG 24 to 18)
Ferrule size	0.25 mm ² or 0.34 mm ² (AWG 24 or 22)

Table A-97 Digital outputs

Technical data	SB 1223 DI 4x5VDC / DQ 4x5VDC
Number of outputs	4, in 1 isolation group of 4 outputs (no isolation outputs to inputs)
Type	Push-pull
Rated voltage	5 V DC
Voltage range	4.25 to 6.0 V DC
Logic 1 signal at max. current	L+ minus 0.7 V
Logic 0 signal at max. current	0.2 V DC max.
Current	0.1 A max.
ON state resistance	7 Ω max.
OFF state resistance	0.2 Ω max.
Pulse Train Output (PTO) rate	200 kHz max., 2 Hz min.
Overload protection	No

Technical data	SB 1223 DI 4x5VDC / DQ 4x5VDC
Isolation (field side to logic)	707 V DC (type test)
Current per common	0.4 A max.
Switching delay	200 ns + 300 ns rise 200 ns + 300 ns fall
Behavior on RUN to STOP	Last value or substitute value (default value 0)
Control of a digital input	Yes
Parallel outputs for redundant load control	No
Parallel outputs for increased load	No
Diagnostics	5 V DC low voltage
Cable length	50 m shielded twisted pair
Cable size	0.2 mm ² to 0.8 mm ² (AWG 24 to 18)
Ferrule size	0.25 mm ² or 0.34 mm ² (AWG 24 or 22)

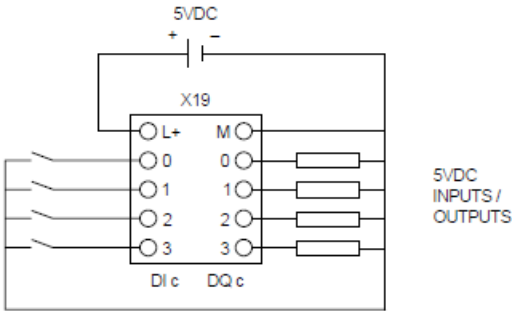
NOTE

When switching frequencies above 20 kHz, you must have a clean square wave. Consider the following options to improve the signal quality:

- Minimize the cable length.
- Change the driver from a sink or source only to a push-pull driver.
- Change to a higher quality cable.
- Add an external load at the input.

Wiring diagram

The wiring diagram and pin connector locations are shown below:

SB 1223 DI 4x5VDC / DQ 4x5VDC				
		X19: Upper User Wiring Terminal (Gray, No Keying)		
		Signal	Pin #	Signal
		L+	1 2	M
		DI c.0	3 4	DQ c.0
		DI c.1	5 6	DQ c.1
		DI c.2	7 8	DQ c.2
		DI c.3	9 10	DQ c.3

A.10 Analog signal boards (SBs)

A.10.1 SB 1231 AI 4x14bit

Table A-98 General specifications

Technical data	SB 1231 AI 4x14bit
Article number	6ES7231-4HD50-0XB0
Dimensions W x H x D	15 x 62 x 63 mm
Weight (product/shipping)	30 grams / 57 grams
Power dissipation	1.4 W
Current consumption (bus)	28 mA max. (5 V DC)
Current consumption (24 V DC)	30 mA
Rated supply voltage	24 V DC
Supply voltage range	20.4 to 28.8 V DC
Reverse supply voltage protection	Yes
Operating environment	Horizontal mounting -20 °C to 40 °C ¹ -20 °C to 60 °C ²
	Vertical mounting -20 °C to 40 °C ¹ -20 °C to 50 °C ²
	95% relative humidity at 25 °C during operation, without condensation, maximum

¹ Operating temperature range using maximum voltages and maximum specifications

² Operating temperature range using rated voltages, 50% of maximum specifications, and alternate I/O active

Table A-99 Analog inputs

Technical data	SB 1231 AI 4x14bit
Number of inputs	4
Type	Voltage or current (differential)
Range	±10 V, ±5 V, ±2.5 V, 0 to 20 mA or 4 to 20 mA
Full scale range (data word)	-27648 to 27648 voltage / 0 to 27648 current
Overshoot/undershoot range (data word)	Voltage: 32511 to 27649 / -27649 to -32512 Current: 32511 to 27649 / 0 to -4864
Overflow/underflow (data word)	Voltage: 32767 to 32512 / -32513 to -32768 Current 0 to 20 mA: 32767 to 32512 / -4865 to -32768 Current 4 to 20 mA: 32767 to 32512 (values below -4864 indicate open wire)
Resolution	13 bits plus sign bit
Maximum withstand voltage/current	±35 V / ±40 mA
Smoothing	None, weak, medium, or strong
Noise rejection	400, 60, 50, or 10 Hz
Input impedance	Before parameterization >= 1 MΩ

¹ The presence of radio frequencies of 500 MHz to 600 MHz can degrade accuracy.

² Voltages outside the operational range applied to one channel can cause interference on other channels.

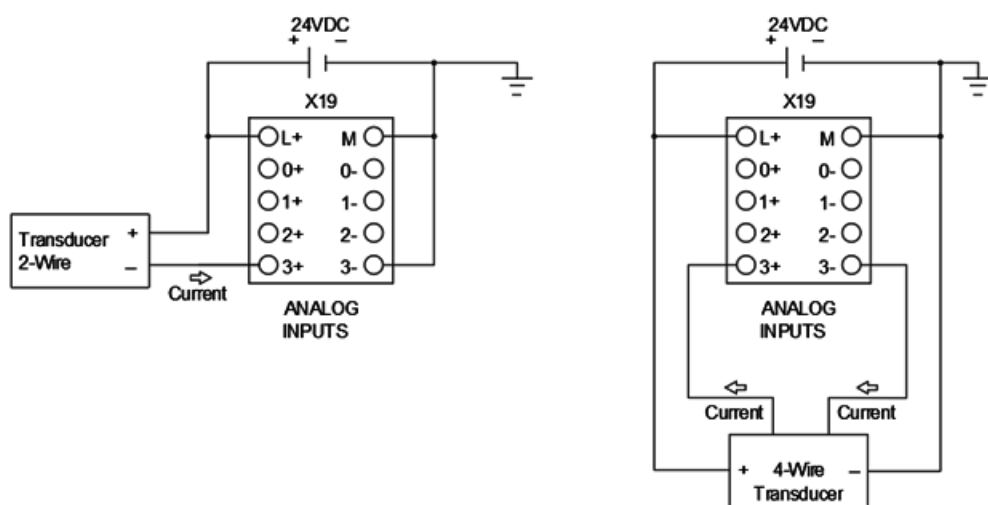
Technical data	SB 1231 AI 4x14bit	
Input impedance	Voltage	$\geq 1 \text{ M}\Omega$
	Current	$< 290 \Omega, > 270 \Omega$
Isolation	Field side to logic	None
	Logic to 24 V DC	None
	Field side to 24 V DC	None
	Channel to channel	None
Accuracy ¹ (25 °C / -20 to 60 °C)	$\pm 0.1\% / \pm 0.2\%$ of full scale	
Measuring principle	Actual value conversion	
Common mode rejection	40 dB, DC to 60 Hz	
Operational signal range ²	Signal plus common mode voltage must be less than +12 V and greater than -12 V	
Diagnostics	Overflow/underflow	
	24 V DC low voltage	
	Open wire, 4 to 20 mA range only (if input is below -4864; 1.185 mA)	
Cable length	100 m, twisted and shielded	
Cable size	0.2 mm ² to 0.8 mm ² (AWG 24 to 18)	
Ferrule size	0.25 mm ² or 0.34 mm ² (AWG 24 or 22)	

¹ The presence of radio frequencies of 500 MHz to 600 MHz can degrade accuracy.

² Voltages outside the operational range applied to one channel can cause interference on other channels.

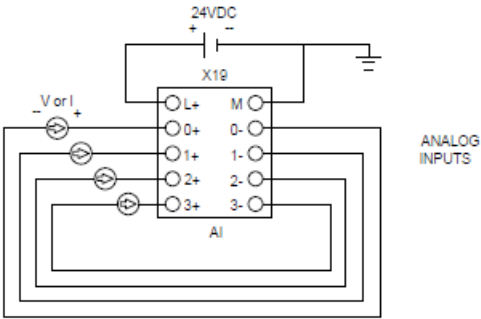
Current measurement

You can implement current measurement with either a 2-wire transducer or a 4-wire transducer as shown below:



Wiring diagram

The wiring diagram and pin connector locations are shown below:

SB 1231 AI 4x14bit			
	X19: Upper user wiring terminal (Light gray, No keying)		
	Signal	Pin #	Signal
	L+	1 2	M
	AI 0+	3 4	AI 0-
	AI 1+	5 6	AI 1-
	AI 2+	7 8	AI 2-
	AI 3+	9 10	AI 3-

NOTE

When wiring and configuring analog input channels consider the following:

- Connect the positive input terminal to the negative input terminal on each unused voltage input channel.
- Set unused current input channels to the 0 to 20 mA range and/or disable broken wire error reporting.

Inputs configured for current mode do not conduct loop current if the module is not powered and configured.

Current input channels are operable only when you supply external power to the transmitter.

A.10.2 SB 1232 AQ 4x14bit

Table A-100 General specifications

Technical data	SB 1232 AQ 4x14bit
Article number	6ES7232-4HD50-0XB0
Dimensions W x H x D	15 x 62 x 63 mm
Weight (product/shipping)	28 grams / 55 grams
Power dissipation	3.0 W
Current consumption (bus)	25 mA max. (5 V DC)
Current consumption (24 V DC)	30 mA
Rated supply voltage	24 V DC
Supply voltage range	20.4 to 28.8 V DC

¹ Operating temperature range using maximum voltages and maximum specifications

² Operating temperature range using rated voltages, 50% of maximum specifications, and alternate I/O active

Technical data	SB 1232 AQ 4x14bit
Reverse supply voltage protection	Yes
Operating environment	Horizontal mounting -20 °C to 40 °C ¹ -20 °C to 60 °C ²
	Vertical mounting -20 °C to 40 °C ¹ -20 °C to 50 °C ²
	95% relative humidity at 25 °C during operation, without condensation, maximum

¹ Operating temperature range using maximum voltages and maximum specifications

² Operating temperature range using rated voltages, 50% of maximum specifications, and alternate I/O active

Table A-101 Analog outputs

Technical data	SB 1232 AQ 4x14bit
Number of outputs	4
Type	Voltage or current
Range	±10 V, 0 to 20 mA, or 4 to 20 mA
Resolution	Voltage: 14 bits Current: 13 bits
Full scale range (data word)	Voltage: -27648 to 27648 Current: 0 to 27648
Accuracy (25 °C / -20 to 60 °C)	±0.3% / ±0.6% of full scale
Settling time (95% of new value)	Voltage: 300 µs (R), 750 µs (1 µF) Current: 600 µs (1 mH), 2 ms (10 mH)
Load impedance	Voltage: ≥ 1000 Ω Current: ≤ 600 Ω
Maximum output short circuit current	Voltage: ≤ 24 mA Current: ≤ 24 mA
Behavior on RUN to STOP	Last value or substitute value (default value 0)
Isolation (field side to logic)	None
Isolation (24 V to output)	None
Diagnostics	Overflow/underflow
	Short to ground (voltage mode only) ¹
	Wire break (current mode only) ²
	24 V DC low voltage
Cable length	100 m, twisted and shielded
Cable size	0.2 mm ² to 0.8 mm ² (AWG 24 to 18)
Ferrule size	0.25 mm ² or 0.34 mm ² (AWG 24 or 22)

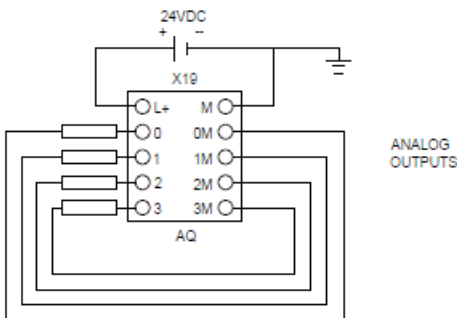
¹ Short circuit detection is only possible when the output voltage is less than -0.5 V or greater than +0.5 V.

² Wire break detection is only possible when the output current is greater than 1 mA.

Wiring diagram

The wiring diagram and pin connector locations are shown below:

SB 1232 AQ 4x14bit



ANALOG
OUTPUTS

X19: Upper User Wiring Terminal (Light Gray, No Keying)

Signal	Pin #		Signal
L+	1	2	M
AQ 0	3	4	AQ 0M
AQ 1	5	6	AQ 1M
AQ 2	7	8	AQ 2M
AQ 3	9	10	AQ 3M

A.10.3 SB 1233 AI 2x14bit / AQ 2x14bit

Table A-102 General specifications

Technical data	SB 1233 AI 2x14bit / AQ 2x14bit
Article number	6ES7233-4HD50-0XB0
Dimensions W x H x D	15 x 62 x 63 mm
Weight (product/shipping)	30 grams / 57 grams
Power dissipation	2.0 W
Current consumption (bus)	29 mA max. (5 V DC)
Current consumption (24 V DC)	25 mA
Rated supply voltage	24 V DC
Supply voltage range	20.4 to 28.8 V DC
Reverse supply voltage protection	Yes
Operating environment	Horizontal mounting -20 °C to 40 °C ¹ -20 °C to 60 °C ²
	Vertical mounting -20 °C to 40 °C ¹ -20 °C to 50 °C ²
	95% relative humidity at 25 °C during operation, without condensation, maximum

¹ Operating temperature range using maximum voltages and maximum specifications

² Operating temperature range using rated voltages, 50% of maximum specifications, and alternate I/O active

Table A-103 Analog inputs

Technical data	SB 1233 AI 2x14bit / AQ 2x14bit	
Number of inputs	2	
Type	Voltage or current (differential)	
Range (Page 475)	± 10 V, ± 5 V, ± 2.5 V, 0 to 20 mA or 4 to 20 mA	
Full scale range (data word)	-27648 to 27648 voltage / 0 to 27648 current	
Overshoot/undershoot range (data word)	Voltage: 32511 to 27649 / -27649 to -32512 Current: 32511 to 27649 / 0 to -4864	
Overflow/underflow (data word)	Voltage: 32767 to 32512 / -32513 to -32768 Current 0 to 20 mA: 32767 to 32512 / -4865 to -32768 Current 4 to 20 mA: 32767 to 32512 (values below -4864 indicate open wire)	
Resolution	13 bits plus sign bit	
Maximum withstand voltage/current	± 35 V / ± 40 mA	
Smoothing	None, weak, medium, or strong	
Noise rejection	400, 60, 50, or 10 Hz	
Input impedance	Before parameterization	≥ 1 M Ω
	Voltage	≥ 1 M Ω
	Current	< 290 Ω , > 270 Ω
Isolation	Field side to logic	None
	Logic to 24 V DC	None
	Field side to 24 V DC	None
	Channel to channel	None
Accuracy (25 °C / -20 to 60 °C)	$\pm 0.1\%$ / $\pm 0.2\%$ of full scale	
Measuring principle	Actual value conversion	
Common mode rejection	40 dB, DC to 60 Hz	
Operational signal range ¹	Signal plus common mode voltage must be less than +12 V and greater than -12 V	
Diagnostics	Overflow/underflow	
	24 V DC low voltage	
	Open wire, 4 to 20 mA range only (if input is below -4864; 1.185 mA)	
Cable length	100 m, twisted and shielded	
Cable size	0.2 mm ² to 0.8 mm ² (AWG 24 to 18)	
Ferrule size	0.25 mm ² or 0.34 mm ² (AWG 24 or 22)	

¹ Voltages outside the operational range applied to one channel can cause interference on other channels.

Table A-104 Analog outputs

Technical data	SB 1233 AI 2x14bit / AQ 2x14bit
Number of outputs	2
Type	Voltage or current
Range (Page 476)	± 10 V, 0 to 20 mA, or 4 to 20 mA

¹ Short circuit detection is only possible when the output voltage is less than -0.5 V or greater than +0.5 V.

² Wire break detection is only possible when the output current is greater than 1 mA.

A.10 Analog signal boards (SBs)

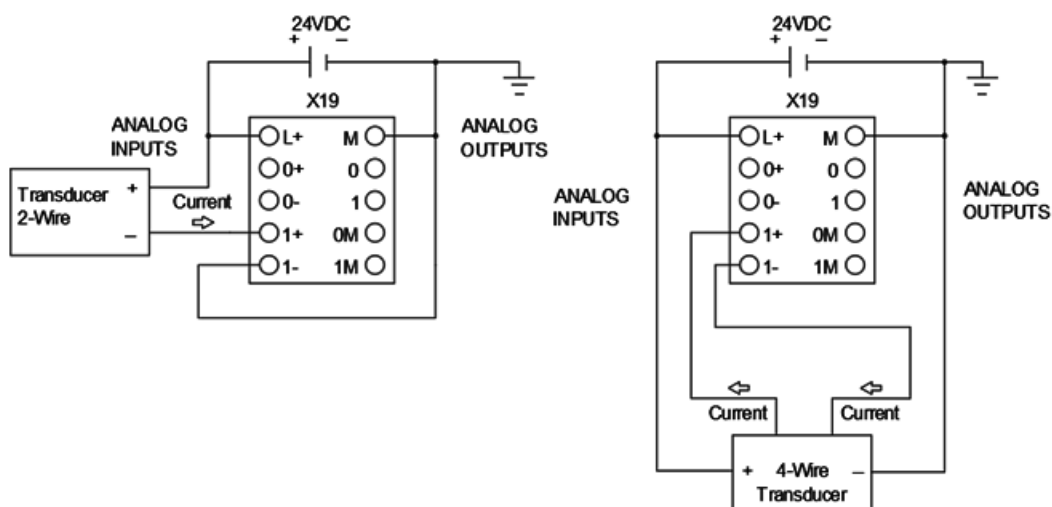
Technical data	SB 1233 AI 2x14bit / AQ 2x14bit
Resolution	Voltage: 14 bits Current: 13 bits
Full scale range (data word)	Voltage: -27648 to 27648 Current: 0 to 27648
Accuracy (25 °C / -20 to 60 °C)	±0.3% / ±0.6% of full scale
Settling time (95% of new value)	Voltage: 300 µs (R), 750 µs (1 µF) Current: 600 µs (1 mH), 2 ms (10 mH)
Load impedance	Voltage: ≥ 1000 Ω Current: ≤ 600 Ω
Maximum output short circuit current	Voltage: ≤ 24 mA Current: ≤ 24 mA
Behavior on RUN to STOP	Last value or substitute value (default value 0)
Isolation (field side to logic)	None
Isolation (24 V to output)	None
Diagnostics	Overflow/underflow
	Short to ground (voltage mode only) ¹
	Wire break (current mode only) ²
	24 V DC low voltage
Cable length	100 m, twisted and shielded
Cable size	0.2 mm ² to 0.8 mm ² (AWG 24 to 18)
Ferrule size	0.25 mm ² or 0.34 mm ² (AWG 24 or 22)

¹ Short circuit detection is only possible when the output voltage is less than -0.5 V or greater than +0.5 V.

² Wire break detection is only possible when the output current is greater than 1 mA.

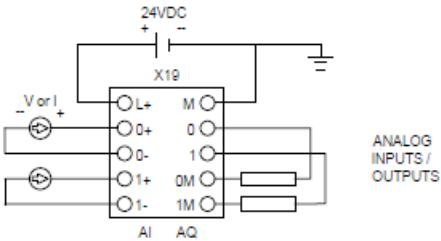
Current measurement

You can implement current measurement with either a 2-wire transducer or a 4-wire transducer as shown below:



Wiring diagram

The wiring diagram and pin connector locations are shown below:

SB 1233 AI 2x14bit / AQ 2x14bit			
	X19: Upper User Wiring Terminal (Light Gray, No Keying)		
	Signal	Pin #	Signal
	L+	1 2	M
	AI 0+	3 4	AQ 0
	AI 0-	5 6	AQ 1
	AI 1+	7 8	AQ 0M
	AI 1-	9 10	AQ 1M

NOTE

When wiring and configuring analog input channels consider the following:

- Connect the positive input terminal to the negative input terminal on each unused voltage input channel.
- Set unused current input channels to the 0 to 20 mA range and/or disable broken wire error reporting.

Inputs configured for current mode do not conduct loop current if the module is not powered and configured.

Current input channels are operable only when you supply external power to the transmitter.

A.10.4 Step response of the analog inputs

Table A-105 Step response (ms), 0 to full scale measured at 95%

Smoothing selection (sample averaging)	Noise reduction/rejection frequency (Integration time selection)			
	400 Hz (2.5 ms)	60 Hz (16.6 ms)	50 Hz (20 ms)	10 Hz (100 ms)
None (1 cycle): No averaging	4 ms	18 ms	22 ms	100 ms
Weak (4 cycles): 4 samples	9 ms	52 ms	63 ms	320 ms
Medium (16 cycles): 16 samples	32 ms	203 ms	241 ms	1200 ms
Strong (32 cycles): 32 samples	61 ms	400 ms	483 ms	2410 ms

A.10.5 Sample time and update times for the analog inputs

Table A-106 Sample time and update times

Rejection frequency (Integration time)	Sample and board update times for all channels			
	400 Hz (2.5 ms)	60 Hz (16.6 ms)	50 Hz (20 ms)	10 Hz (100 ms)
2 or 4 channels	0.625 ms	4.17 ms	5 ms	25 ms

A.10.6 Measurement ranges of the analog inputs for voltage and current

Table A-107 Analog input representation for voltage

System		Voltage measuring range				
Decimal	Hexadecimal	+/- 10 V	+/- 5 V	+/- 2.5 V	+/- 1.25 V	
32767	7FFF ¹	11.851 V	5.926 V	2.963 V	1.481 V	Overflow
32512	7F00					
32511	7EFF	11.759 V	5.879 V	2.940 V	1.470 V	Overshoot range
27649	6C01					
27648	6C00	10 V	5 V	2.5 V	1.250 V	Rated range
20736	5100	7.5 V	3.75 V	1.875 V	0.938 V	
1	1	361.7 μ V	180.8 μ V	90.4 μ V	45.2 μ V	
0	0	0 V	0 V	0 V	0 V	
-1	FFFF					
-20736	AF00	-7.5 V	-3.75 V	-1.875 V	-0.938 V	
-27648	9400	-10 V	-5 V	-2.5 V	-1.250 V	Under-shoot range
-27649	93FF					
-32512	8100	-11.759 V	-5.879 V	-2.940 V	-1.470 V	Underflow
-32513	80FF					
-32768	8000	-11.851 V	-5.926 V	-2.963 V	-1.481 V	

¹ The channel can return 7FFF for one of the following reasons: overflow (as noted in this table), before valid values are available (for example, immediately upon a power up), or if a wire break is detected.

Table A-108 Analog input representation for current

System		Current measuring range		
Decimal	Hexadecimal	0 mA to 20 mA	4 mA to 20 mA	
32767	7FFF	> 23.52 mA	> 22.81 mA	Overflow
32511	7EFF	23.52 mA	22.81 mA	Overshoot range
27649	6C01			
27648	6C00	20 mA	20 mA	Nominal range
20736	5100	15 mA	16 mA	
1	1	723.4 nA	4 mA + 578.7 nA	
0	0	0 mA	4 mA	

¹ The wire break value of 32767 (16#7FFF) is always returned regardless of the state of the wire break alarm.

System		Current measuring range		
Decimal	Hexadecimal	0 mA to 20 mA	4 mA to 20 mA	
-1	FFFF			Undershoot range
-4864	ED00	-3.52 mA	1.185 mA	
32767 ¹	7FFF		< 1.185 mA	Wire break (4 to 20 mA)
-32768	8000	< -3.52 mA		Underflow (0 to 20 mA)

¹ The wire break value of 32767 (16#7FFF) is always returned regardless of the state of the wire break alarm.

A.10.7 Measurement ranges of the analog outputs for voltage and current

Table A-109 Analog output representation for voltage

System		Voltage output range	
Decimal	Hexadecimal	+/- 10 V	
32767	7FFF	See note 1	Overflow
32512	7F00	See note 1	
32511	7EFF	11.76 V	Overshoot range
27649	6C01		
27648	6C00	10 V	Rated range
20736	5100	7.5 V	
1	0001	361.7 μ V	
0	0000	0 V	
-1	FFFF	-361.7 μ V	
-20736	AF00	-7.5 V	
-27648	9400	-10 V	
-27649	93FF		Undershoot range
-32512	8100	-11.76 V	
-32513	80FF	See note 1	Underflow
-32768	8000	See note 1	

¹ In an overflow or underflow condition, analog outputs take on the substitute value of the STOP mode.

Table A-110 Analog output representation for current

System		Current output range		
Decimal	Hexadecimal	0 mA to 20 mA	4 mA to 20 mA	
32767	7FFF	See note 1	See note 1	Overflow
32512	7F00	See note 1	See note 1	
32511	7EFF	23.52 mA	22.81 mA	Overshoot range
27649	6C01			
27648	6C00	20 mA	20 mA	Rated range
20736	5100	15 mA	16 mA	
1	1	723.4 nA	4 mA + 578.7 nA	

¹ In an overflow or underflow condition, analog outputs take on the substitute value of the STOP mode.

System		Current output range		
Decimal	Hexadecimal	0 mA to 20 mA	4 mA to 20 mA	
0	0	0 mA	4 mA	Rated range
-1	FFFF		4 mA to 578.7 nA	Undershoot range
-6912	E500		0 mA	
-6913	E4FF			
-32512	8100			Not possible. Output value limited to 0 mA.
-32513	80FF			
-32768	8000	See note 1	See note 1	
		See note 1	See note 1	Underflow

¹ In an overflow or underflow condition, analog outputs take on the substitute value of the STOP mode.

A.10.8 Basic operation of a thermocouple

A thermocouple is formed whenever two dissimilar metals are electrically bonded to each other. A voltage is generated across the bonded junction that is proportional to the junction temperature. This voltage is small; one microvolt could represent many degrees. Measuring the voltage from a thermocouple, compensating for extra junctions, and then linearizing the result forms the basis of temperature measurement using thermocouples.

The place where the two dissimilar wires are attached to each other forms the sensor thermocouple. The other ends of the thermocouple wires are each attached to a module or board at the signal connector.

Two more thermocouples are formed where the two wires are attached to the signal connector. The connector temperature causes a voltage that adds to the voltage from the sensor thermocouple. If this voltage is not corrected, then the temperature reported will deviate from the sensor temperature.

Cold junction compensation is used to compensate for the connector thermocouples. Thermocouple tables are based on a reference junction temperature, usually zero degrees Celsius. The cold junction compensation compensates the connector to zero degrees Celsius.

The cold junction compensation restores the voltage added by the connector thermocouples. The temperature of the module or board is measured internally, and then converted to a value to be added to the sensor conversion. The corrected sensor conversion is then linearized using the thermocouple tables.

For optimum operation of the cold junction compensation, the thermocouple module or board must be located in a thermally stable environment. Slow variation (less than 0.1 °C/minute) in ambient temperature is correctly compensated within the module or board specifications. Air movement across the module or board will also cause cold junction compensation errors.

If better cold junction error compensation is needed, an external iso-thermal terminal block can be used. The thermocouple board provides for use of a 0 °C referenced or 50 °C referenced terminal block.

A.10.9 SB 1231 AI 4xTC

Table A-111 General specifications

Technical data	SB 1231 AI 4xTC
Article number	6ES7231-5QD50-0XB0
Dimensions W x H x D	15 x 62 x 63 mm
Weight (product/shipping)	29 grams / 56 grams
Power dissipation	0.4 W
Current consumption (bus)	65 mA max. (5 V DC)
Current consumption (24 V DC)	None
Operating environment	Horizontal mounting
	-20 °C to 40 °C ¹
	-20 °C to 60 °C ²
	Vertical mounting
	-20 °C to 40 °C ¹
	-20 °C to 50 °C ²
	95% relative humidity at 25 °C during operation, without condensation, maximum

¹ Operating temperature range using maximum voltages and maximum specifications

² Operating temperature range using rated voltages, 50% of maximum specifications, and alternate I/O active

Table A-112 Analog inputs

Technical data	SB 1231 AI 4xTC	
Number of inputs	4	
Sensor types	J, K, T, E, R & S, B, N, C, TXK/XK(L), voltage	
Ranges	See Selection tables for thermocouple sensors.	
Resolution	Temperature	0.1 °C / 0.1 °F
	Voltage	15 bits plus sign
Maximum withstand voltage	±35 V	
Noise rejection	85 dB for selected filter setting (10 Hz, 50 Hz, 60 Hz or 400 Hz)	
Common mode rejection	> 120 dB at 120 V AC	
Impedance	≥ 10 MΩ	
Isolation	Field side to logic	707 V DC (type test)
	Logic to 24 V DC	707 V DC (type test)
	Field side to 24 V DC	707 V DC (type test)
	Channel to channel	120 V AC
Accuracy	See Selection tables for thermocouple sensors.	
Repeatability	±0.05% of full scale	
Measuring principle	Integrating	

¹ The overflow and underflow diagnostic alarm information is reported in the analog data values even if the alarms are disabled in the board configuration.

² When wire break alarm is disabled and an open wire condition exists in the sensor wiring, the board can report random values.

³ The board performs wire break testing every 6 seconds, which extends the update time by 9 ms for each enabled channel once every 6 seconds.

Technical data	SB 1231 AI 4xTC
Board update time	See Noise reduction and update times for the Thermocouple board.
Cold junction error (Page 477)	± 1.5 °C
Wire resistance	100 Ω max.
Diagnostics	Overflow/underflow ¹
	Wire break ^{2, 3}
Cable length	100 m to sensor max.
Cable size	0.2 mm ² to 0.8 mm ² (AWG 24 to 18)
Ferrule size	0.25 mm ² or 0.34 mm ² (AWG 24 or 22)

¹ The overflow and underflow diagnostic alarm information is reported in the analog data values even if the alarms are disabled in the board configuration.

² When wire break alarm is disabled and an open wire condition exists in the sensor wiring, the board can report random values.

³ The board performs wire break testing every 6 seconds, which extends the update time by 9 ms for each enabled channel once every 6 seconds.

The SB 1231 Thermocouple (TC) analog signal board measures the value of voltage connected to the board inputs. The temperature measurement type can be either "Thermocouple" or "Voltage".

- "Thermocouple": The value is reported in degrees multiplied by ten. (For example, 25.3 degrees is reported as decimal 253).
- "Voltage": The nominal range full scale value is decimal 27648.

Selection tables for thermocouple sensors

Table A-113 Thermocouple selection table

Type	Under-range minimum ¹	Nominal range low limit	Nominal range high limit	Over-range maximum ²	Normal range accuracy @ 25 °C ³	Normal range accuracy -20 °C to 60 °C ^{1, 2, 5}
J	-210.0 °C -346.0 °F	-150.0 °C -238.0 °F	1200.0 °C 2192.0 °F	1450.0 °C 2642.0 °F	± 0.3 °C ± 0.5 °F	± 1.2 °C ± 2.2 °F
K	-270.0 °C -454.0 °F	-200.0 °C -328.0 °F	1372.0 °C 2501.6 °F	1622.0 °C 2951.6 °F	± 0.4 °C ± 0.7 °F	± 2.0 °C ± 3.6 °F
T	-270.0 °C -454.0 °F	-200.0 °C -328.0 °F	400.0 °C 752.0 °F	540.0 °C 1004.0 °F	± 0.5 °C ± 0.9 °F	± 1.0 °C ± 1.8 °F
E	-270.0 °C -454.0 °F	-200.0 °C -328.0 °F	1000.0 °C 1832.0 °F	1200.0 °C 2192.0 °F	± 0.3 °C ± 0.5 °F	± 0.6 °C ± 1.1 °F

¹ Thermocouple values below the under-range minimum value are reported as -32768.

² Thermocouple values above the over-range maximum value are reported as 32767.

³ Internal cold junction error is ± 1.5 °C for all ranges. This adds to the error in this table. The board requires at least 30 minutes of warm-up time to meet this specification. For board ambient temperatures below -10 °C, internal cold junction error can be greater than 1.5 °C.

⁴ Lower limit of 3276.6 °F with °F reporting

⁵ Cold junction compensation error has not been characterized for board ambient temperatures below 0 °C, and can exceed the specified value.

A.10 Analog signal boards (SBs)

Type	Under-range minimum ¹	Nominal range low limit	Nominal range high limit	Over-range maximum ²	Normal range accuracy @ 25 °C ³	Normal range accuracy -20 °C to 60 °C ^{1, 2, 5}
R & S	-50.0 °C -58.0 °F	100.0 °C 212.0 °F	1768.0 °C 3214.4 °F	2019.0 °C 3276.6 °F ⁴	±1.0 °C ±1.8 °F	±2.5 °C ±4.5 °F
B	0.0 °C 32.0 °F -- --	200.0 °C 392.0 °F 800.0 °C 1472.0 °F	800.0 °C 1472.0 °F 1820.0 °C 3276.6 °F ⁴	-- -- 1820.0 °C 3276.6 °F ⁴	±2.0 °C ±3.6 °F ±1.0 °C ±1.8 °F	±2.5 °C ±4.5 °F ±2.3 °C ±4.1 °F
N	-270.0 °C -454.0 °F	-200.0 °C -328.0 °F	1300.0 °C 2372.0 °F	1550.0 °C 2822.0 °F	±1.0 °C ±1.8 °F	±1.6 °C ±2.9 °F
C	0.0 °C 32.0 °F	100.0 °C 212.0 °F	2315.0 °C 3276.6 °F ⁴	2500.0 °C 3276.6 °F ⁴	±0.7 °C ±1.3 °F	±4.5 °C ±8.1 °F
TXK/XK(L)	-200.0 °C -328.0 °F	-150.0 °C 302.0 °F	800.0 °C 1472.0 °F	1050.0 °C 1922.0 °F	±0.6 °C ±1.1 °F	±1.2 °C ±2.2 °F
Voltage	-32512	-27648 -80mV	27648 80mV	32511	±0.05%	±0.1%

¹ Thermocouple values below the under-range minimum value are reported as -32768.

² Thermocouple values above the over-range maximum value are reported as 32767.

³ Internal cold junction error is ±1.5 °C for all ranges. This adds to the error in this table. The board requires at least 30 minutes of warm-up time to meet this specification. For board ambient temperatures below -10 °C, internal cold junction error can be greater than 1.5 °C.

⁴ Lower limit of 3276.6 °F with °F reporting

⁵ Cold junction compensation error has not been characterized for board ambient temperatures below 0 °C, and can exceed the specified value.

NOTE

You can configure each channel on the Thermocouple signal board with a different thermocouple type (selectable in the software during configuration of the board).

Table A-114 Noise reduction and update times for the Thermocouple board

Rejection frequency selection	Integration time	Board update time (seconds)
400 Hz (2.5 ms)	10 ms ¹	0.285
60 Hz (16.67 ms)	16.67 ms	0.445
50 Hz (20 ms)	20 ms	0.525
10 Hz (100 ms)	100 ms	2.450

¹ To maintain resolution and accuracy when the 400 Hz filter is selected, the integration time is 10 ms. This selection also rejects 100 Hz and 200 Hz noise.

Siemens recommends using a 100 ms integration time for measuring thermocouples. The use of smaller integration times increases the repeatability error of the temperature readings.

Internal calibration

After power is applied, the board performs internal calibration for the analog-to-digital converter. During this time, the board reports a value of 32767 on each channel until the channel provides valid data. The STEP 7 program might need to allow for this initialization time. Because the initialization time varies based on the board's configuration, you must verify the behavior of the board in your system. If required, you can include logic in the STEP 7 program to accommodate the initialization time of the board.

You can implement this logic using a polling read in the "Startup OB" which blocks operation until the initialization is complete. You must implement the polling read with an immediate access. If the value of the thermocouple polling read is 32767, you must repeat the read until the value changes. For each board, use only the input channel with the greatest value for the thermocouple polling read. For example, if input channel number 2 is the highest used input channel, you should execute the thermocouple polling read on channel number 2. The board initializes the channels in order from 0 to 3.

Representation of analog values for Thermocouple Type J

A representation of the analog values of thermocouple type J is shown in the table below:

Table A-115 Representation of analog values of thermocouple type J

Type J in °C ¹	Units		Type J in °F ¹	Units		Range
	Decimal	Hexadecimal		Decimal	Hexadecimal	
> 1450.0	32767	7FFF	> 2642.0	32767	7FFF	Overflow
1450.0	14500	38A4	2642.0	26420	6734	Over-range
⋮	⋮	⋮	⋮	⋮	⋮	
1200.1	12001	2EE1	2192.2	21922	55A2	Rated range
1200.0	12000	2EE0	2192.0	21920	55A0	
⋮	⋮	⋮	⋮	⋮	⋮	
-150	1500	FA24	-238.0	-2380	F6B4	
-150.1	-1501	FA23	-238.1	-2381	F6B3	Under-range
⋮	⋮	⋮	⋮	⋮	⋮	
-210	-2100	F7CC	-346.0	-3460	F27C	Underflow ²
< -210.0	-32768	8000	< -346.0	-32768	8000	

¹ A value change of 1 indicates a temperature change of +/- one-tenth degree.

² Faulty wiring (for example, polarity reversal, or open inputs) or sensor error in the negative range (for example, wrong type of thermocouple) can cause the thermocouple module to signal underflow.

Wiring diagram

The wiring diagram and pin connector locations are shown below:

SB 1231 AI 4xTC

X19

0+	0-
1+	1-
2+	2-
3+	3-

AI

ANALOG INPUTS

①

+

-

X19: Upper user wiring terminal (Light gray, No keying)

Signal	Pin #		Signal
AI 0+	1	2	AI 0-
AI 1+	3	4	AI 1-
AI 2+	5	6	AI 2-
AI 3+	7	8	AI 3-
	9	10	

① TC 0, 1, and 2 are not shown connected for clarity.

NOTE
Connect the positive input terminal to the negative input terminal on each unused TC input channel. You can deactivate unused thermocouple channels. Deactivated channels do not report errors.

A.10.10 SB 1231 AI 2xRTD

Table A-116 General specifications

Technical data	SB 1231 AI 2xRTD
Article number	6ES7231-5PB50-0XB0
Dimensions W x H x D	15 x 62 x 63 mm
Weight (product/shipping)	29 grams / 56 grams
Power dissipation	0.3 W
Current consumption (bus)	50 mA max. (5 V DC)
Current consumption (24 V DC)	None
Operating environment	Horizontal mounting -20 °C to 40 °C ¹ -20 °C to 60 °C ²
	Vertical mounting -20 °C to 40 °C ¹ -20 °C to 50 °C ²
	95% relative humidity at 25 °C during operation, without condensation, maximum

¹ Operating temperature range using maximum voltages and maximum specifications

² Operating temperature range using rated voltages, 50% of maximum specifications, and alternate I/O active

Table A-117 Analog inputs

Technical data	SB 1231 AI 2xRTD	
Number of inputs	2	
Sensor types	See Selection table for RTD sensors.	
Ranges	See Selection table for RTD sensors.	
Resolution	Temperature	0.1 °C / 0.1 °F
	Resistance	15 bits plus sign
Maximum withstand voltage	±35 V	
Noise rejection	85 dB for the selected noise reduction (10 Hz, 50 Hz, 60 Hz or 400 Hz)	
Common mode rejection	> 120 dB	
Impedance	≥ 10 MΩ	
Isolation	Field side to logic	707 V DC (type test)
	Logic to 24 V DC	707 V DC (type test)
	Field side to 24 V DC	707 V DC (type test)
	Channel to channel	None
Accuracy	See Selection table for RTD sensors. ⁴	
Repeatability	±0.05% of full scale	
Maximum sensor dissipation	0.2 mW	
Measuring principle	Integrating	
Board update time	See Noise reduction and update times for the RTD board.	
Wire resistance	20 Ω, 2.7 Ω for 10 Ω RTD max.	
Diagnostics	Overflow/underflow ^{1, 2}	
	Wire break ³	
Cable length	100 m to sensor max.	
Cable size	0.2 mm ² to 0.8 mm ² (AWG 24 to 18)	
Ferrule size	0.25 mm ² or 0.34 mm ² (AWG 24 or 22)	

¹ The overflow and underflow diagnostic alarm information is reported in the analog data values, even if the alarms are disabled in the board configuration.

² For resistance ranges, underflow detection is never enabled.

³ When wire break alarm is disabled and an open wire condition exists in the sensor wiring, the board can report random values.

⁴ Accuracy can be affected when the signal board is subjected to radio frequency radiation between 480 MHz to 800 MHz or when the signal board's ambient temperature changes at a rate of 3 °C per minute or faster.

The SB 1231 AI 2xRTD measures the value of resistance connected to the signal board inputs. The measurement type can be selected as either "Resistor" or "Thermal resistor".

- "Resistor": The nominal range full scale value is decimal 27648.
- "Thermal resistor": The value is reported in degrees multiplied by ten. (For example, 25.3 degrees is reported as decimal 253.) The climatic range values are reported in degrees multiplied by one hundred. (For example, 25.34 degrees is reported as decimal 2534.)

The SB 1231 AI 2xRTD uses a current to measure the resistance of the sensor. For resistance ranges and the RTD ranges of 200 ohms or less the current is 0.25 mA. For the 500- and 1000-ohm RTD ranges the current is 0.20 mA. This current is pulsed depending on the

number of active channels on the module. For two active channels, the duty cycle for one channel is 50%. If four channels are active, the duty cycle for one channel is 25%. The maximum output voltage for an open circuit condition on the sensor is 3.3 V DC (measured between the I+ and I- terminals).

The SB 1231 AI 2xRTD supports measurements with 2-wire, 3-wire, and 4-wire connections to the sensor resistor.

Selection table for RTD sensors

Table A-118 Ranges and accuracy for the different sensors supported by the RTD board

Temperature coefficient	RTD type	Under range minimum ¹	Nominal range low limit	Nominal range high limit	Over range maximum ²	Normal range accuracy @ 25 °C	Normal range accuracy -20 °C to 60 °C
Pt 0.003850 ITS90 DIN EN 60751	Pt 100 climatic	-145.00 °C	-120.00 °C	145.00 °C	155.00 °C	±0.20 °C	±0.40 °C
	Pt 10	-243.0 °C	-200.0 °C	850.0 °C	1000.0 °C	±1.0 °C	±2.0 °C
	Pt 50	-243.0 °C	-200.0 °C	850.0 °C	1000.0 °C	±0.5 °C	±1.0 °C
	Pt 100						
	Pt 200						
	Pt 500						
	Pt 1000						
Pt 0.003902 Pt 0.003916 Pt 0.003920	Pt 100	-243.0 °C	-200.0 °C	850.0 °C	1000.0 °C	±0.5 °C	±1.0 °C
	Pt 200						
	Pt 500						
	Pt 1000						
Pt 0.003910	Pt 10	-273.2 °C	-240.0 °C	1100.0 °C	1295.0 °C	±1.0 °C	±2.0 °C
	Pt 50	-273.2 °C	-240.0 °C	1100.0 °C	1295.0 °C	±0.8 °C	±1.6 °C
	Pt 100						
	Pt 500						
Ni 0.006720 Ni 0.006180	Ni 100	-105.0 °C	-60.0 °C	250.0 °C	295.0 °C	±0.5 °C	±1.0 °C
	Ni 120						
	Ni 200						
	Ni 500						
	Ni 1000						
LG-Ni 0.005000	LG-Ni 1000	-105.0 °C	-60.0 °C	250.0 °C	295.0 °C	±0.5 °C	±1.0 °C
Ni 0.006170	Ni 100	-105.0 °C	-60.0 °C	180.0 °C	212.4 °C	±0.5 °C	±1.0 °C
Cu 0.004270	Cu 10	-240.0 °C	-200.0 °C	260.0 °C	312.0 °C	±1.0 °C	±2.0 °C
Cu 0.004260	Cu 10	-60.0 °C	-50.0 °C	200.0 °C	240.0 °C	±1.0 °C	±2.0 °C
	Cu 50	-60.0 °C	-50.0 °C	200.0 °C	240.0 °C	±0.6 °C	±1.2 °C
	Cu 100						

¹ RTD values below the under-range minimum value are reported as -32768.

² RTD values above the over-range maximum value are reported as +32767.

Temperature coefficient	RTD type	Under range minimum ¹	Nominal range low limit	Nominal range high limit	Over range maximum ²	Normal range accuracy @ 25 °C	Normal range accuracy -20 °C to 60 °C
Cu 0.004280	Cu 10	-240.0 °C	-200.0 °C	200.0 °C	240.0 °C	±1.0 °C	±2.0 °C
	Cu 50	-240.0 °C	-200.0 °C	200.0 °C	240.0 °C	±0.7 °C	±1.4 °C
	Cu 100						

¹ RTD values below the under-range minimum value are reported as -32768.

² RTD values above the over-range maximum value are reported as +32767.

Table A-119 Resistance

Range	Under range minimum	Nominal range low limit	Nominal range high limit	Over range maximum ¹	Normal range accuracy @ 25 °C	Normal range accuracy -20 °C to 60 °C
150 Ω	n/a	0 (0 Ω)	27648 (150 Ω)	176.383 Ω	±0.05%	±0.1%
300 Ω	n/a	0 (0 Ω)	27648 (300 Ω)	352.767 Ω	±0.05%	±0.1%
600 Ω	n/a	0 (0 Ω)	27648 (600 Ω)	705.534 Ω	±0.05%	±0.1%

¹ Resistance values above the over-range maximum value are reported as +32767.

The board reports 32767 on any activated channel with no sensor connected. If open wire detection is also enabled, the board flashes the appropriate red LEDs.

When 500 Ω and 1000 Ω RTD ranges are used with other lower value resistors, the error can increase to two times the specified error.

Best accuracy is achieved for the 10 Ω RTD ranges if 4 wire connections are used.

The resistance of the connection wires in 2 wire mode causes an error in the sensor reading; therefore, accuracy is not guaranteed.

Table A-120 Noise reduction and update times for the RTD board

Rejection frequency selection	Integration time	Board update time (seconds)
400 Hz (2.5 ms)	10 ms ¹	4- / 2-wire: 0.142 3-wire: 0.285
60 Hz (16.67 ms)	16.67 ms	4- / 2-wire: 0.222 3-wire: 0.445
50 Hz (20 ms)	20 ms	4- / 2-wire: 0.262 3-wire: 0.505
10 Hz (100 ms)	100 ms	4- / 2-wire: 1.222 3-wire: 2.445

¹ To maintain resolution and accuracy when the 400 Hz filter is selected, the integration time is 10 ms. This selection also rejects 100 Hz and 200 Hz noise.

Internal calibration

After power is applied, the board performs internal calibration for the analog-to-digital converter. During this time, the board reports a value of 32767 on each channel until the channel provides valid data. The STEP 7 program might need to allow for this initialization time. Because the initialization time varies based on the board's configuration, you must verify the behavior of the board in your system. If required, you can include logic in the STEP 7 program to accommodate the initialization time of the board.

You can implement this logic using a polling read in the "Startup OB" which blocks operation until the initialization is complete. You must implement the polling read with an immediate access. If the value of the RTD polling read is 32767, you must repeat the read until the value changes. For each board, use only the input channel with the greatest value for the RTD polling read. For example, if input channel number 0 is the highest used input channel, you should execute the RTD polling read on channel number 0. The board initializes the channels in order from 0 to 1.

Representation of analog values for RTDs

A representation of the digitized measured value for the RTD standard temperature range sensors is shown in the table below:

Table A-121 Representation of analog values for resistance temperature detectors PT 100, 200, 500, 1000 and PT 10, 50, 100, 500 GOST (0.003850) standard

Pt x00 standard in °C ¹	Units		Pt x00 standard in °F ¹	Units		Range
	Decimal	Hexadecimal		Decimal	Hexadecimal	
> 1000.0	32767	7FFF	> 1832.0	32767	7FFF	Overflow
1000.0 : 850.1	10000 : 8501	2710 : 2135	1832.0 : 1562.1	18320 : 15621	4790 : 3D05	Over-range
850.0 : -200.0	8500 : -2000	2134 : F830	1562.0 : -328.0	15620 : -3280	3D04 : F330	Rated range
-200.1 : -243.0	-2001 : -2430	F82F : F682	-328.1 : -405.4	-3281 : -4054	F32F : F02A	Under-range
< -243.0	-32768	8000	< -405.4	-32768	8000	Underflow

¹ A value change of 1 indicates a temperature change of +/- one-tenth degree.

Wiring diagram

The wiring diagram and pin connector locations are shown below:

SB 1231 AI 2xRTD

The diagram shows terminal block X19 with pins 1 through 10. Pins 1 and 2 are for AI I0+, pins 3 and 4 for AI I0-. Pins 5 and 6 for AI M0+, pins 7 and 8 for AI M0-. Pins 9 and 10 are unused. Below the terminal block, four RTD connection types are shown: 1-wire loop back (labeled 1), 2-wire (labeled 2), 3-wire (labeled 3), and 4-wire (labeled 4). The text 'ANALOG INPUTS' is also present.

X19: Upper user wiring terminal (Light gray, No keying)

Signal	Pin #		Signal
AI I0+	1	2	AI I1+
AI I0-	3	4	AI I1-
AI M0+	5	6	AI M1+
AI M0-	7	8	AI M1-
	9	10	

- ① Loop back unused inputs.
- ② 2-wire RTD connection represented.
- ③ 3-wire RTD connection represented.
- ④ 4-wire RTD connection represented.

NOTE

You can deactivate unused RTD channels. Deactivated channels do not report errors.

To avoid extra stabilization time, which is automatically added to an active unused channel, make the current loop continuous. For consistency, connect a resistor like the 2-wire RTD connection to the RTD board.

A.11 Battery board (BB) 1297

The S7-1200 G2 Battery board (BB) 1297 provides long-term backup of the real-time clock. It is pluggable in the signal board slot(s) of the S7-1200 G2 CPU. You must add the battery board to the device configuration and download the hardware configuration to the CPU for the battery board to be functional. The battery is not included and must be purchased separately. When adding or replacing the battery, a UL certified CR2032 (Li/MnO₂) battery with a rating of 3 V, 225 mAh must be used.

WARNING

Risks when installing or connecting an unspecified battery in the BB 1297

Installing an unspecified battery in the battery board or otherwise connecting an unspecified battery to the circuit can result in fire or component damage and unpredictable operation of machinery. The battery must be installed in a non-hazardous environment.

Use only the specified battery for backup of the real-time clock.

Fire or unpredictable operation of machinery can result in death, severe personal injury, or property damage.

Table A-122 General specifications

Technical data	BB 1297
Article number	6ES7297-4AX50-0XA0
Dimensions W x H x D (mm)	15 x 62 x 63 mm
Weight (product/shipping)	26 grams / 42 grams
Power dissipation	0.2 W
Current consumption (SM Bus)	35 mA max. (5 V DC)
Current consumption (24 V DC)	None
Operating environment	Horizontal mounting -20 °C to 40 °C ¹ -20 °C to 60 °C ²
	Vertical mounting -20 °C to 40 °C ¹ -20 °C to 50 °C ²
	95% relative humidity at 25 °C during operation, without condensation, maximum

¹ Operating temperature range using maximum voltages and maximum specifications

² Operating temperature range using rated voltages, 50% of maximum specifications, and alternate I/O active

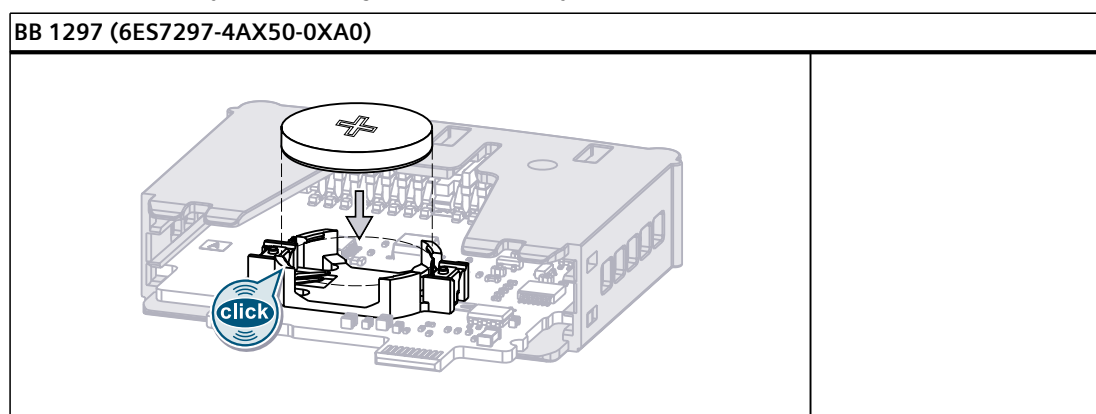
Battery (not included)	BB 1297
Hold up time	Approximately 1 year
Battery type	CR2032, temperature rating of ≥ 85 °C recommended
Nominal voltage	3 V
Nominal capacity	At least 200 mAh

Diagnostics	BB 1297
Critical battery level	< 2.5 V ¹
Battery diagnostic	Low voltage indicator: ² - Low battery voltage causes the CPU MAINT LED to illuminate with the yellow light continuously ON. - Diagnostic buffer event: 16#06:2700 "Maintenance demanded: At least one battery empty"
Battery status	You can use input bit Ic.0 in the STEP 7 program to monitor the battery status. 0 = Battery OK 1 = Battery low
Battery status update	Battery status updates at power up and then once per day while CPU is in RUN mode.

¹ If the battery charge is 2.5 V or less, it triggers the diagnostic buffer event 16#06:2700 and causes the yellow light of the CPU MAINT LED to be continuously lit. The CPU can maintain the real-time clock until the battery charge is 1.1 V or less. At this point, the real-time clock loads a default date and time (UTC Jan 1, 2012 00:00) because the value could be inaccurate.

² The battery only powers the real-time clock. The deterioration of the battery does not affect the retentive memory.

Table A-123 Battery insertion diagram for the battery board



A.12 Communication interfaces

A.12.1 CP 1243-1

Table A-124 General specifications

Technical data	CP 1243-1
Article number	6GK7243-1BX50-0XE0
Dimensions W x H x D	30 x 134 x 100 mm
Weight (product/shipping)	180 grams / 230 grams
Power dissipation	1.7 W
Current consumption (bus)	0 mA (24 V DC external power supply)
Current consumption (24 V DC)	70 mA
Rated supply voltage	24 V DC

Technical data	CP 1243-1
Supply voltage range	19.2 to 28.8 V DC
Reverse supply voltage protection	Yes
Operating environment	Horizontal mounting -20 °C to 70 °C
	Vertical mounting -20 °C to 60 °C
	95% relative humidity at 25 °C during operation, without con- densation, maximum

Table A-125 Properties

Technical data	CP 1243-1
Ethernet	Yes

For additional information, see CP 1243-1 (<https://sieportal.siemens.com/su/blYx6>).

Wiring diagram

The wiring diagram and pin connector locations are shown below:

CP 1243-1

The diagram shows a terminal block with two rows of three terminals each. The top row is labeled '24VDC POWER' and the bottom row is labeled '24VDC OUTPUTS'. A 24VDC power source is connected to the top row terminals. The bottom row terminals are connected to a common ground. The terminals are labeled L+, M, and an unlabeled terminal.

X80: DC power wiring terminal (Gray, No keying)

DC power	L+		M
Pin #	1	3	5
Pin#	2	4	6
24 V DC output	GND	L+	M

A.12.2 CM 1241 RS232/422/485

Table A-126 General specifications

Technical data	CM 1241 RS232/422/485
Article number	6ES7241-1EA50-0XB0
Dimensions W x H x D	30 x 125 x 100 mm
Weight (product/shipping)	178 grams / 215 grams
Power dissipation	0.9 W
Current consumption (bus)	170 mA max. (5 V DC)
Current consumption (24 V DC)	None
Operating environment	Horizontal mounting -20 °C to 60 °C ¹
	Vertical mounting -20 °C to 50 °C ¹
	95% relative humidity at 25 °C during operation, without condensation, maximum

¹ Operating temperature range using maximum voltages and maximum specifications

NOTE

The CM 1241 supports three configuration types: RS232, RS422, and RS485. You can only use one configuration type per CM; you cannot use these configuration types simultaneously on the same CM. However, you can configure each CM in the G2 system with a different type.

Table A-127 Transmitter and receiver for CM 1241 RS232/422/485 when configured as RS232

Technical data	CM 1241 RS232/422/485	
Type	RS232 (full duplex)	
Parity	No parity (default), even, odd, Mark (parity bit always set to 1), Space (parity bit always set to 0)	
Number of stop bits	1 (default), 2	
Wait time	0 to 65535 ms	
Data transmission rate	300, 600, 1200, 2400, 4800, 9600 (default), 19200, 38400, 57600, 76800, 115200 bits/s	
Transmitter output voltage	±5 V min. at $R_L = 3 \text{ k}\Omega$	
Transmit output voltage	±15 V DC max.	
Receiver input impedance	3 kΩ min.	
Receiver threshold/sensitivity	0.8 V min. low, 2.4 max. high; 0.5 V typical hysteresis	
Isolation	RS232 signal to chassis ground	707 V DC (type test)
	RS232 signal to CPU logic common	707 V DC (type test)
Receiver input voltage	±25 V DC max.	
Flow control	Hardware, software	
Cable length	10 m shielded max.	
Cable size	0.2 mm ² to 1.5 mm ² (AWG 24 to 16)	

Table A-128 Transmitter and receiver for CM 1241 RS232/422/485 when configured as RS422/485

Technical data	CM 1241 RS232/422/485	
Type	RS422 (full duplex) or RS485	
Parity	No parity (default), even, odd, Mark (parity bit always set to 1), Space (parity bit always set to 0)	
Number of stop bits	1 (default), 2	
Wait time	0 to 65535 ms	
Data transmission rate	300, 600, 1200, 2400, 4800, 9600 (default), 19200, 38400, 57600, 76800, 115200, 250000 bits/s	
Common mode voltage range	RS422: -7 V to +12 V, 1 second, 3 VRMS continuous	
Transmitter differential output voltage	2 V min. at $R_L = 100 \Omega$ 1.5 V min. at $R_L = 54 \Omega$	
Termination and bias (Page 278)	Internal bias options provided, including none. Optional 300 Ω internal termination provided. No external termination required.	
Receiver input impedance	5.4 k Ω min. including termination	
Receiver threshold/sensitivity	± 0.2 V min., 60 mV typical hysteresis	
Isolation	RS422/485 signal to chassis ground	707 V DC (type test)
	RS422/485 signal to CPU logic common	707 V DC (type test)
Flow control	RS422: XON/XOFF	
Cable length	1000 m shielded max. (data transmission rate dependent)	
Cable size	0.2 mm ² to 1.5 mm ² (AWG 24 to 16)	

Wiring diagram

The wiring diagram and pin connector locations are shown below:

CM 1241 RS232/422/485				
		X30: Upper user wiring terminal (Gray, No keying)		
		RS232 Signal	Pin #	RS232 Signal
		DSR Data set ready	1 2	DTR Data terminal ready
		RxD Receive data	3 4	TxD Transmit data
		CTS Clear to send	5 6	RTS Request to send
		DCD Data carrier detect	7 8	M Logic or comm ground
		RI Ring indicator	9 10	
		X31: Lower user wiring terminal (Gray, No keying)		
		RS485 Signal	Pin #	RS422 Signal

① 300 Ω termination can be made by connecting pin 7 to pin 9 on the X31 terminal block (recommended when cable length is greater than 50 m).

CM 1241 RS232/422/485					
		B Data (+) Signal B (Rx/D/TxD+)	1	2	Rb Receive Data (+) Signal B (Rx/D+)
		A Data (-) Signal A (Rx/D/TxD-)	3	4	Ra Receive Data (-) Signal A (Rx/D-)
		M Logic or comm ground	5	6	M Logic or comm ground
		See ①	7	8	Tb Transmit Data (+) Signal B (Tx/D+)
		See ①	9	10	Ta Transmit Data (-) Signal A (Tx/D-)

① 300 Ω termination can be made by connecting pin 7 to pin 9 on the X31 terminal block (recommended when cable length is greater than 50 m).

A.12.3 CB 1241 RS485

Table A-129 General specifications

Technical data	CB 1241 RS485
Article number	6ES7241-1CA50-0XB0
Dimensions W x H x D	15 x 62 x 63 mm
Weight (product/shipping)	29 grams / 56 grams
Power dissipation	0.4 W
Current consumption (bus)	75 mA max. (5 V DC)
Current consumption (24 V DC)	None

¹ Operating temperature range using maximum voltages and maximum specifications

Technical data	CB 1241 RS485
Operating environment	Horizontal mounting -20 °C to 60 °C ¹
	Vertical mounting -20 °C to 50 °C ¹
	95% relative humidity at 25 °C during operation, without condensation, maximum

¹ Operating temperature range using maximum voltages and maximum specifications

Table A-130 Transmitter and receiver

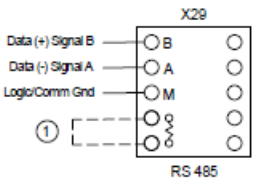
Technical data	CB 1241 RS485	
Type	RS485	
Data transmission rate	300, 600, 1200, 2400, 4800, 9600 (default), 19200, 38400, 57600, 76800, 115200, 250000 bits/s	
Parity	No parity (default), even, odd, Mark (parity bit always set to 1), Space (parity bit always set to 0)	
Number of stop bits	1 (default), 2	
Wait time	0 to 65535 ms	
Common mode voltage range	-7 V to +12 V, 1 second, 3 VRMS continuous	
Transmitter differential output voltage	2 V min. at $R_L = 100 \Omega$ 1.5 V min. at $R_L = 54 \Omega$	
Termination and bias	Internal bias options provided, including none. Optional 300 Ω internal termination provided. No external termination required.	
Receiver input impedance	5.4 k Ω min. including termination	
Receiver threshold/sensitivity	± 0.2 V min., 60 mV typical hysteresis	
Isolation	RS485 signal to chassis ground	707 V DC (type test)
	RS485 signal to CPU logic common	707 V DC (type test)
Flow control	Not supported	
Cable length	1000 m shielded max. (data transmission rate dependent)	
Cable size	0.2 mm ² to 0.8 mm ² (AWG 24 to 18)	
Ferrule size	0.25 mm ² or 0.34 mm ² (AWG 24 or 22)	

Wiring diagram

The wiring diagram and pin connector locations are shown below:

CB 1241 RS485				
		X29: Upper user wiring terminal (Gray, No keying)		
		RS485 Signal	Pin #	

① 300 Ω termination can be made by connecting pin 7 to pin 9 on the X29 terminal block (recommended when cable length is greater than 50 m).

CB 1241 RS485					
		B Data (+) Signal B (Rx/D/TxD+)	1	2	
		A Data (-) Sig- nal A (Rx/D/TxD-)	3	4	
		M Logic or comm ground	5	6	
		See ①	7	8	
		See ①	9	10	

① 300 Ω termination can be made by connecting pin 7 to pin 9 on the X29 terminal block (recommended when cable length is greater than 50 m).

A.13 Input simulators

Table A-131 General specifications

Technical data	8 Position Simulator	14 Position Simulator
Article number	6ES7274-1XF50-0XA0	6ES7274-1XH50-0XA0
Dimensions W x H x D (mm)	43 x 35 x 23	67 x 35 x 23
Weight	20 grams	30 grams
Points	8	14
Used with CPU	CPU 1212C, CPU 1212FC	CPU 1214C, CPU 1214FC

WARNING

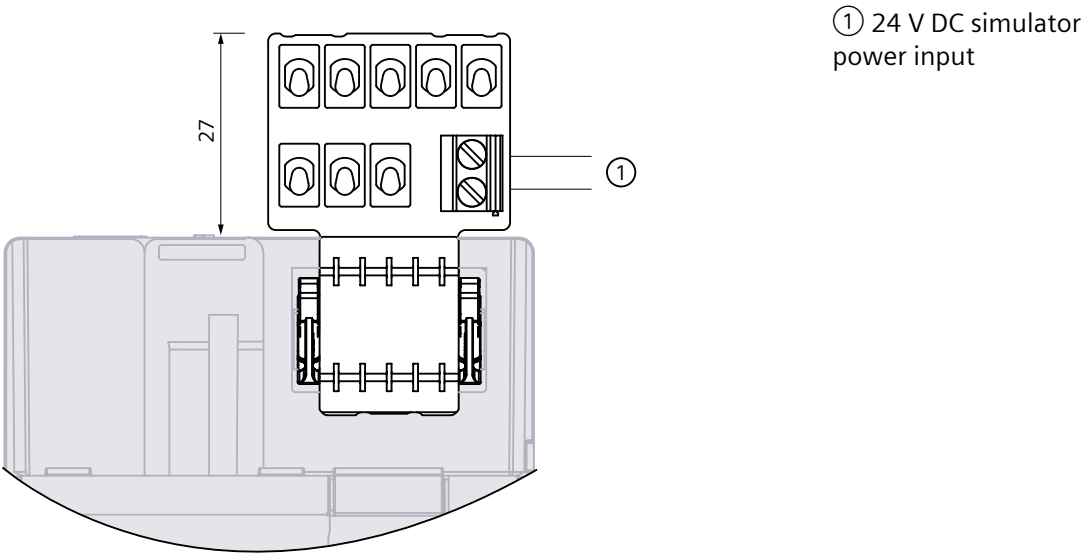
Safe use of input simulators

Input simulators are not approved for use in Class I DIV 2 or Class I Zone 2 hazardous locations where they present a potential hazard.

Do not use in Class I DIV 2 or Class I Zone 2 hazardous locations.

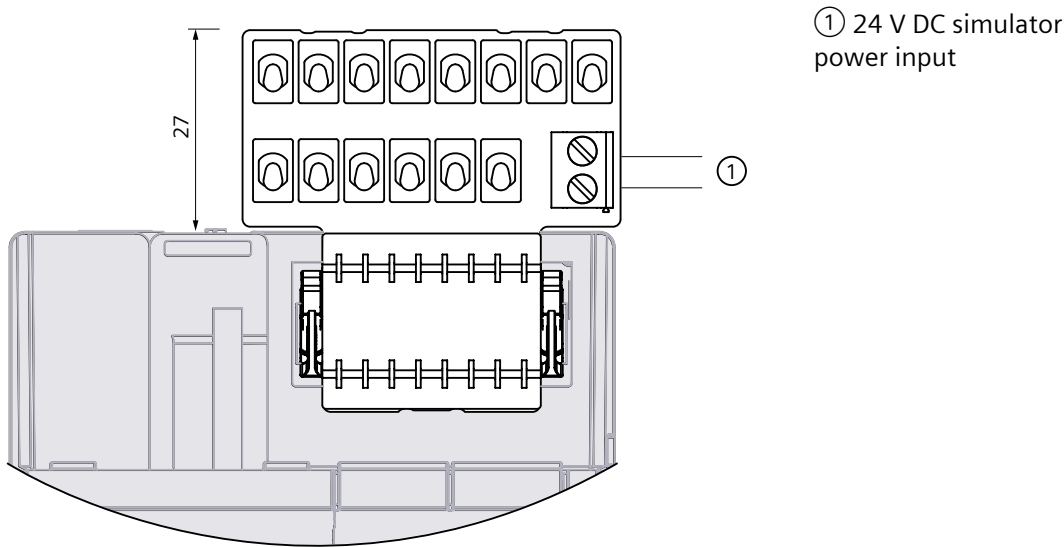
Unapproved use can result in death or severe personal injury, and property damage.

8 Position Simulator (6ES7274-1XF50-0XA0)



All dimensions are in millimeters (mm).

14 Position Simulator (6ES7274-1XH50-0XA0)



All dimensions are in millimeters (mm).

See also

[Mounting dimensions \(Page 67\)](#)

A.14 Companion products

A.14.1 Power module (PM) 1207

The PM 1207 is an optional external power supply for the SIMATIC S7-1200 G2 system.

Technical data	PM 1207
Article number	6EP3333-4SC00-3AX0 (with EX certification) 6EP3333-4SB00-3AX0 (without EX certification)
Dimensions W x H x D	70 x 125 x 100 mm
Weight (product/shipping)	450 grams / 600 grams
Design format	Matches the S7-1200 G2 shape and color
Input	120 to 240 V AC
Voltage range	85 to 264 V AC
Line frequency	47 to 63 Hz
Input current (full load)	1.1 A at 120 V AC 0.56 A at 240 V AC
Inrush current	43 A max. at 240 V AC
$I^2 t$	1.8 A ² s
Isolation (input AC to output DC)	3000 V AC
Hold up time (loss of power)	20 ms at 120 V AC 85 ms at 240 V AC
Internal fuse	3.15 A, slow blow, not user replaceable
External miniature circuit breaker recommended	16 A characteristic B or 10 A characteristic C
Output	24 V DC / 5A
UDI diagnostic interface	Yes
Power dissipation	13 W
Current consumption (bus)	Not connected to CPU bus
Operating environment	Horizontal mounting -25 °C to 60 °C ¹
	Vertical mounting -25 °C to 50 °C ¹
	95% relative humidity at 25 °C during operation, without condensation, maximum
Cable size	0.2 mm ² to 1.5 mm ² (AWG 24 to 16)

¹ Operating temperature range using maximum voltages and maximum specifications

You can find more information about this module on the product catalog
(<https://support.industry.siemens.com/cs/us/en/ps>) web site.

Ordering information

B.1 CPUs

Table B-1 CPUs

CPU models		Article number
CPU 1212C	CPU 1212C AC/DC/RLY	6ES7212-1BG50-0XB0
	CPU 1212C DC/DC/DC	6ES7212-1AG50-0XB0
	CPU 1212C DC/DC/RLY	6ES7212-1HG50-0XB0
CPU 1214C	CPU 1214C AC/DC/RLY	6ES7214-1BH50-0XB0
	CPU 1214C DC/DC/DC	6ES7214-1AH50-0XB0
	CPU 1214C DC/DC/RLY	6ES7214-1HH50-0XB0

Table B-2 Fail-safe CPUs

Fail-safe CPU models		Article number
CPU 1212FC	CPU 1212FC DC/DC/DC	6ES7212-1AF50-0XB0
	CPU 1212FC DC/DC/RLY	6ES7212-1HF50-0XB0
CPU 1214FC	CPU 1214FC DC/DC/DC	6ES7214-1AF50-0XB0
	CPU 1214FC DC/DC/RLY	6ES7214-1HF50-0XB0

B.2 Signal modules (SMs)

Signal modules (SMs)		Article number
Digital input	SM 1221 DI 16x24VDC	6ES7221-1BH50-0XB0
Digital output	SM 1222 DQ 16x24VDC	6ES7222-5BH50-0XB0
	SM 1222 DQ 16xRLY	6ES7222-5HH50-0XB0
Digital input / output	SM 1223 DI 8x24VDC / DQ 8x24VDC	6ES7223-5BH50-0XB0
	SM 1223 DI 8x24VDC / DQ 8xRLY	6ES7223-5PH50-0XB0
	SM 1223 DI 16x24VDC / DQ 16x24VDC	6ES7223-5BL50-0XB0
	SM 1223 DI 16x24VDC / DQ 16x24VDC Sink	6ES7223-5BL50-1XB0
	SM 1223 DI 16x24VDC / DQ 16xRLY	6ES7223-5PL50-0XB0
Analog input	SM 1231 AI 8x14bit	6ES7231-4HF50-0XB0
Analog output	SM 1232 AQ 8x14bit	6ES7232-4HF50-0XB0
Analog input / output	SM 1233 AI 4x14bit / AQ 4x14bit	6ES7233-4HF50-0XB0
RTD and thermo-couple	SM 1231 AI 8xTC	6ES7231-5QF50-0XB0
	SM 1231 AI 4xRTD	6ES7231-5PD50-0XB0

B.3 Signal boards (SBs)

Signal boards (SBs)		Article number
Digital input	SB 1221 DI 8x24VDC	6ES7221-3BF50-0XB0
Digital output	SB 1222 DQ 8x24VDC	6ES7222-5BF50-0XB0
Digital input / output	SB 1223 DI 4x24VDC / DQ 4x24VDC	6ES7223-7BF50-0XB0
	SB 1223 DI 4x5VDC / DQ 4x5VDC	6ES7223-7AF50-0XB0
Analog input	SB 1231 AI 4x14bit	6ES7231-4HD50-0XB0
Analog output	SB 1232 AQ 4x14bit	6ES7232-4HD50-0XB0
Analog input / output	SB 1233 AI 2x14bit / AQ 2x14bit	6ES7233-4HD50-0XB0
RTD and thermocouple	SB 1231 AI 4xTC	6ES7231-5QD50-0XB0
	SB 1231 AI 2xRTD	6ES7231-5PB50-0XB0

B.4 Battery board (BB)

Battery board (BB)		Article number
Battery	BB 1297 (battery type CR2032 not included)	6ES7297-4AX50-0XA0

B.5 Communication

Table B-3 Communication processor (CP)

Communication processor (CP)		Article number
Ethernet interface	CP 1243-1	6GK7243-1BX50-0XE0

Table B-4 Communication module (CM)

Communication module (CM)		Article number
Serial communication	CM 1241 RS232/422/485	6ES7241-1EA50-0XB0

Table B-5 Communication board (CB)

Communication board (CB)		Article number
Serial communication	CB 1241 RS485	6ES7241-1CA50-0XB0

B.6 Memory cards

SIMATIC memory cards	Description	Article number
Siemens SIMATIC MC	32 GB	6ES7954-8LT0x-0AA0
	2 GB	6ES7954-8LP0x-0AA0
	256 MB	6ES7954-8LL0x-0AA0
	24 MB	6ES7954-8LF0x-0AA0
	12 MB	6ES7954-8LE0x-0AA0
	4 MB	6ES7954-8LC0x-0AA0

Standard memory cards ¹	Description	Vendor part number ²
INDMEM	512 MB, Type SDHC	B0CVVRFQ4
	1 GB, Type SDHC	B0CVVR1W9T
Transcend	4 GB, Type SDHC	TS4GSDHC4
	8 GB, Type SDHC	TS8GSDC300S
Verbatim	4 GB, Type SDHC	B000RLBWJK
	8 GB, Type SDHC	B000WJ725U
	16 GB, Type SDHC	B001L1RGUE
SanDisk	16 GB, Type SDHC	SDSDBNN-016G-AW6VN
	32 GB, Type SDHC	SDSQUA4-032G-AW6KA
Onn	32 GB, Type SDHC	100006056

¹ You can only use Standard (non-SIMATIC) memory cards for transferring the license conditions and copyrights Open Source Software (OSS) information to a memory card for viewing.

² These devices are not sold by Siemens. Other memory cards of type SDHC may also work.

B.7 Spare parts and other hardware

Table B-6 Simulators, spare doors, DIN rails, and end retainer

Item		Article number
Input simulator	Input simulator, 8 position (CPU 1212C, CPU 1212FC)	6ES7274-1XF50-0XA0
	Input simulator, 14 position (CPU 1214C, CPU 1214FC)	6ES7274-1XH50-0XA0
Spare door kit (one pair per kit)	CPU 1212C, CPU 1212FC (70 mm)	6ES7291-1AA50-0XA0
	CPU 1214C, CPU 1214FC (80 mm)	6ES7291-1AB50-0XA0
	SM, CM (30 mm)	6ES7291-1BA50-0XA0
	SM (50 mm)	6ES7291-1BB50-0XA0
DIN rail	DIN rail 35 mm, length 483 mm	6ES5710-8MA11
	DIN rail 35 mm, length 530 mm	6ES5710-8MA21
	DIN rail 35 mm, length 830 mm	6ES5710-8MA31
	DIN rail 35 mm, length 2000 mm	6ES5710-8MA41
DIN rail end retain- er	End retainer thermoplastic, 5.2 mm	8WH9150-0CA00

B.8 Terminal block spare kits

Replacing the terminal block connector

Refer to the tables below and your module specifications to determine the correct terminal block replacement.

NOTE

PLCs require correct wiring to ensure safety and proper operation.

When replacing the terminal block in your S7-1200 G2 CPU or module, it is important that you use the correct terminal block and correct wiring source for your module.

The G2 removable terminal block is designed to prevent you from accidentally placing a high voltage wired terminal block into a low voltage module, or from placing a special voltage wired terminal block into a normal voltage module.

Table B-7 CPU - Terminal block spare kits

CPU (article number)	Use this terminal block spare kit (four per pack)	
	Terminal block description	Terminal block article number
CPU 1212C DC/DC/DC (6ES7212-1AG50-0XB0)	6 position, tin-plated, gray	6ES7292-2AF50-0XA0
	8 position, tin-plated, gray	6ES7292-2AH50-0XA0
	10 position, tin-plated, gray	6ES7292-2AK50-0XA0
CPU 1212C DC/DC/RLY (6ES7212-1HG50-0XB0)	6 position, tin-plated, gray	6ES7292-2AF50-0XA0
	8 position, tin-plated, orange	6ES7292-2AH50-0XA3
	10 position, tin-plated, gray	6ES7292-2AK50-0XA0
CPU 1212C AC/DC/RLY (6ES7212-1BG50-0XB0)	6 position, tin-plated, orange	6ES7292-2AF50-0XA3
	8 position, tin-plated, orange	6ES7292-2AH50-0XA3
	10 position, tin-plated, gray	6ES7292-2AK50-0XA0
CPU 1214C DC/DC/DC (6ES7214-1AH50-0XB0)	6 position, tin-plated, gray	6ES7292-2AF50-0XA0
	12 position, tin-plated, gray	6ES7292-2AM50-0XA0
	16 position, tin-plated, gray	6ES7292-2AR50-0XA0
CPU 1214C DC/DC/RLY (6ES7214-1HH50-0XB0)	6 position, tin-plated, gray	6ES7292-2AF50-0XA0
	12 position, tin-plated, orange	6ES7292-2AM50-0XA3
	16 position, tin-plated, gray	6ES7292-2AR50-0XA0
CPU 1214C AC/DC/RLY (6ES7214-1BH50-0XB0)	6 position, tin-plated, orange	6ES7292-2AF50-0XA3
	12 position, tin-plated, orange	6ES7292-2AM50-0XA3
	16 position, tin-plated, gray	6ES7292-2AR50-0XA0

Table B-8 Fail-safe CPU - Terminal block spare kit

Fail-safe CPU (article number)	Use this terminal block spare kit (four per pack)	
	Terminal block description	Terminal block article number
CPU 1212FC DC/DC/DC (6ES7212-1AF50-0XB0)	6 position, tin-plated, gray	6ES7292-2AF50-0XA0
	8 position, tin-plated, gray	6ES7292-2AH50-0XA0
	10 position, tin-plated, gray	6ES7292-2AK50-0XA0
CPU 1212FC DC/DC/RLY (6ES7212-1HF50-0XB0)	6 position, tin-plated, gray	6ES7292-2AF50-0XA0
	8 position, tin-plated, orange	6ES7292-2AH50-0XA3

B.8 Terminal block spare kits

Fail-safe CPU (article number)	Use this terminal block spare kit (four per pack)	
	Terminal block description	Terminal block article number
CPU 1212FC DC/DC/RLY (6ES7212-1HF50-0XB0)	10 position, tin-plated, gray	6ES7292-2AK50-0XA0
CPU 1214FC DC/DC/DC (6ES7214-1AF50-0XB0)	6 position, tin-plated, gray	6ES7292-2AF50 0XA0
	12 position, tin-plated, gray	6ES7292-2AM50-0XA0
	16 position, tin-plated, gray	6ES7292-2AR50-0XA0
CPU 1214FC DC/DC/RLY (6ES7214-1HF50-0XB0)	6 position, tin-plated, gray	6ES7292-2AF50 0XA0
	12 position, tin-plated, orange	6ES7292-2AM50-0XA3
	16 position, tin-plated, gray	6ES7292-2AR50-0XA0

Table B-9 SM - Terminal block spare kits

SM (article number)	Use this terminal block spare kit (four per pack)	
	Terminal block description	Terminal block article number
SM 1221 DI 16x24VDC (6ES7221-1BH50-0XB0)	10 position, tin-plated, gray	6ES7292-2AK50-0XA0
SM 1222 DQ 16x24VDC (6ES7222-5BH50-0XB0)	10 position, tin-plated, gray	6ES7292-2AK50-0XA0
SM 1222 DQ 16xRLY (6ES7222-5HH50-0XB0)	14 position, tin-plated, orange	6ES7292-2AP50-0XA3
SM 1223 DI 8x24VDC / DQ 8x24VDC (6ES7223-5BH50-0XB0)	10 position, tin-plated, gray	6ES7292-2AK50-0XA0
SM 1223 DI 16x24VDC / DQ 16x24VDC (6ES7223-5BL50-0XB0)		
SM 1223 DI 16x24VDC / DQ 16x24VDC Si- nk (6ES7223-5BL50-1XB0)		
SM 1223 DI 8x24VDC / DQ 8xRLY (6ES7223-5PH50-0XB0)	10 position, tin-plated, gray 14 position, tin-plated, orange	6ES7292-2AK50-0XA0 6ES7292-2AP50-0XA3
SM 1223 DI 16x24VDC / DQ 16xRLY (6ES7223-5PL50-0XB0)		
SM 1231 AI 8x14bit (6ES7231-4HF50-0XB0)	10 position, gold-plated, light gray	6ES7292-2BK50-0XA4
SM 1232 AQ 8x14bit (6ES7232-4HF50-0XB0)		
SM 1233 AI 4x14bit / AQ 4x14bit (6ES7233-4HF50-0XB0)		
SM 1231 AI 8xTC (6ES7231-5QF50-0XB0)	10 position, gold-plated, light gray	6ES7292-2BK50-0XA4
SM 1231 AI 4xRTD (6ES7231-5PD50-0XB0)		

Table B-10 CM - Terminal block spare kits

CM (article number)	Use this terminal block spare kit (four per pack)	
	Terminal block description	Terminal block article number
CM 1241 RS232/422/485 (6ES7241-1EA50-0XB0)	10 position, tin-plated, gray	6ES7292-2AK50-0XA0

Table B-11 SB - Terminal block spare kits

SB (article number)	Use this terminal block spare kit (four per pack)	
	Terminal block description	Terminal block article number
SB 1221 DI 8x24VDC (6ES7221-3BF50-0XB0)	10 position, tin-plated, gray	6ES7292-4AK50-0XA0
SB 1222 DQ 8x24VDC (6ES7222-5BF50-0XB0)		
SB 1223 DI 4x24VDC / DQ 4x24VDC (6ES7223-7BF50-0XB0)		
SB 1223 DI 4x5VDC / DQ 4x5VDC (6ES7223-7AF50-0XB0)		
SB 1231 AI 4x14bit (6ES7231-4HD50-0XB0)	10 position, gold plated, light gray	6ES7292-4BK50-0XA4
SB 1232 AQ 4x14bit (6ES7232-4HD50-0XB0)		
SB 1233 AI 2x14bit / AQ 2x14bit (6ES7233-4HD50-0XB0)		
SB 1231 AI 4xTC (6ES7231-5QD50-0XB0)		
SB 1231 AI 2xRTD (6ES7231-5PB50-0XB0)		

Table B-12 CB - Terminal block spare kits

CB (article number)	Use this terminal block spare kit (four per pack)	
	Terminal block description	Terminal block article number
CB 1241 RS485 (6ES7241-1CA50-0XB0)	10 position, tin-plated, gray	6ES7292-4AK50-0XA0

Table B-13 CP - Terminal block spare kits

CP (article number)	Use this terminal block spare kit (four per pack)	
	Terminal block description	Terminal block article number
CP 1243-1 (6GK7243-1BX50-0XE0)	6 position, tin-plated, gray	6ES7292-2AF50-0XA0

B.9 Programming software

Table B-14 Programming software

SIMATIC software		Article number
Programming software	STEP 7 Basic V20	6ES7822-0AE24-0YA5
	STEP 7 Professional V20	6ES7822-1AE24-0YA5

Safety-relevant symbols

C.1 Devices without explosion protection

The following table explains the symbols located on your SIMATIC device, on its packaging, or in the accompanying documentation:

Symbol	Meaning
	General warning sign Caution/Notice Read the product documentation. The product documentation contains information about potential risks and enables you to recognize these risks and to implement countermeasures.
	Read the information provided by the product documentation. ISO 7010 M002
	Ensure the device is only installed by an electrically skilled person. IEC 60417 No. 6182
 CABLE SPEC.	Connected mains lines must be designed according to the expected minimum and maximum ambient temperature.
 EMC	The device must be constructed and connected in accordance with EMC regulations.
 230V MODULES	A 230 V device can be exposed to electrical voltages, which can be dangerous. ANSI Z535.2
 24V MODULES	A device of Protection Class III can only be supplied with a protective low voltage according to the standard SELV/PELV. IEC 60417-1-5180 "Class III equipment"
 INDOOR USE ONLY INDUSTRIAL USE ONLY	The device is only approved for the industrial field and only for indoor use.
	An enclosure is required for installing the device. The following are considered to be enclosures: • Standing control cabinet • Modular control cabinet • Terminal boxes • Wall enclosure

C.2 Devices with explosion protection

The following table explains the symbols located on your SIMATIC device, on its packaging, or in the accompanying documentation:

Symbol	Meaning
	General warning sign Caution/Notice Read the product documentation. The product documentation contains information about potential risks and enables you to recognize these risks and to implement countermeasures.
	The assigned safety symbol applies to devices with Ex approval . Read the product documentation. The product documentation contains information about potential risks and enables you to recognize these risks and to implement countermeasures.
	Read the information provided by the product documentation. ISO 7010 M002
	Ensure the device is only installed by an electrically skilled person. IEC 60417 No. 6182
 F<2N DISPLAY F<4N HOUSING	Observe the mechanical rating of the device.
 CABLE SPEC.	Connected mains lines must be designed according to the expected minimum and maximum ambient temperature.
 EMC	The device must be constructed and connected in accordance with EMC regulations.
 U = 0V	When the device is under voltage, it cannot be installed or removed, or plugged or pulled.
 230V MODULES	A 230 V device can be exposed to electrical voltages, which can be dangerous. ANSI Z535.2
 24V MODULES	A device of Protection Class III can only be supplied with a protective low voltage according to the standard SELV/PELV. IEC 60417-1-5180 "Class III equipment"

Symbol	Meaning
 INDOOR USE ONLY INDUSTRIAL USE ONLY	The device is only approved for the industrial field and only for indoor use.
 ZONE 2 INSIDE CABINET IP54	For Zone 2 potentially explosive atmospheres, the device can only be used when it is installed in an enclosure with a degree of protection $\geq$ IP54.
 ZONE 22 INSIDE CABINET IP6x	For Zone 22 potentially explosive atmospheres, the device can only be used when it is installed in an enclosure with a degree of protection $\geq$ IP6x.

Comparison to S7-1200

The following tables represent a comparison between S7-1200 and S7-1200 G2:

Major features	S7-1200	S7-1200 G2
Web API Support (Page 316)	Yes (subset)	Yes
Maximum number of concurrent Web API sessions	50	30
Mobile phone NFC Application (Page 315)	No	Yes
DHCP	No	Yes
DNS	No	Yes
OPC UA Server	Yes	Yes
Numerous Communication Modules:		
• PROFIBUS	Yes	No
• AS-I Master	Yes	No
• LTE (US and EU)	Yes	No
Configuration control (option handling)	Yes	No
S7 Routing	Yes	Yes

Features	S7-1200	S7-1200 G2
CPU Variants	1211C, 1212C, 1214C, 1215C, 1217C, 1212FC, 1214FC, 1215FC	1212C 1214C 1212FC 1214FC
Physical Dimensions, W x H x D (mm)	CPU 1211C/1212C: 90 x 100 x 75 CPU 1214C: 110 x 100 x 75 CPU 1215C: 130 x 100 x 75 CPU 1217C: 150 x 100 x 75 SM: 45 or 70 x 100 x 75 CM/CP: 30 x 100 x 75 SB/CB: 38 x 62 x 21	CPU 1212C/1212FC: 70 x 125 x 100 CPU 1214C/1214FC: 80 x 125 x 100 SM/CM: 30 or 50 x 125 x 100 SB/CB: 15 x 62 x 63
Built-in Analog	Yes	No, analog SMs (Page 433) and SBs (Page 466) available
Signal Boards Slots	1 for all CPU variants	CPU 1212C/1212FC: 1 CPU 1214C/1214FC: 2
SM/CM/CP	CPU 1211C: 3 CM/CP / 0 SM CPU 1212C: 3 CM/CP / 2 SM CPU 1214C/1215C/1217C: 3 CM/CP / 8 SM	CPU 1212C/1212FC: 6 total, 3 can be CMs or CPs CPU 1214C/1214FC: 10 total, 3 can be CMs or CPs

Features	S7-1200	S7-1200 G2
Module Placement	Left side (CM/CPs) Right side (SMs)	Right side only (CMs/CPs must be next to CPU)
Security (Page 166)	Standard Security Measures	Enhanced Security
Number of Ethernet Ports	CPU 1211C/1212C/1214C: 1 port (one interface) CPU 1215C/1217C: 2 switched ports (one interface)	All CPUs: 2 switched ports (one interface)
Load Memory Reporting (Online & diagnostics)	Load memory only reports program blocks	Reports the size of everything
IRT (Isochronous Real-Time PN) (Page 265)	No Support	HW Support
RT (Real-Time PN)	SW Support	HW Support
Motion Control (Page 318)	Yes	Yes (different)
Number of PROFINET Devices (Page 234)	16	31
Communication Priority	1 (will not interrupt 2 and above)	15 (will not interrupt 16 and above)
Memory Card Evaluation (what happens when you plug a memory card (Page 144))	Evaluates on transition to RUN, power up, and memory reset (MRES)	Evaluates on insertion, power up, and memory reset (MRES)
Work Memory Reporting	Work Memory (includes both code and data)	Code Work Memory / Data Work Memory
Cyclic OB (Page 106) (TIA cycle configuration)	milliseconds	microseconds
Synchronous Isochronous Interrupt OB 61	Cyclic only	Tied to Isochronous Scan
Programming Error OB 121 (Page 121) (synchronous)	No	Yes
I/O Access Error OB 122 (Page 122) (synchronous)	No	Yes
Number of User PIP(s) (Page 101)	4	32
Number of Diagnostics buffer (Page 133) Events		
- Visible in the buffer - Retentive	50 50	500 100
Reaction after serious firmware or hardware exception	Attempts defect-mode restart; LEDs show fatal error flash pattern	Attempts defect-mode restart (Page 336); attempts to load device configuration and program; LEDs (Page 331) show fatal error flash pattern;
Alarming configure, display, acknowledge		
- Program alarm wizard - PLC alarms editor - Alarm display - PLC alarm text lists - Central alarm management	No No No Yes No	Yes Yes Yes Yes Yes
Local output substitute values during startup	System automatically sets the output image	System automatically sets the output image

Features	S7-1200	S7-1200 G2
Distributed output substitute values during startup	User must use startup OB to set	User must use startup OB to set
Process image size	1 Kbyte inputs 1 Kbyte outputs	1 Kbyte inputs 1 Kbyte outputs
Bit memory size	8 Kbytes	8 Kbytes
Retentive Memory	14KB	20KB
TIA Languages	LAD, FBD, SCL, and CEM	LAD, FBD, SCL, and CEM
Media Redundancy Protocol (MRP) Support	Yes	Yes
Media Redundancy for Planned Duplication (MRPD) Support	No	Yes
TIA Portal Power Budget Calculation for local rack	No	Yes
Insertion or extraction of modules under power (hot swap)	No	No
EN 60068-2-6 Sinusoidal vibration	DIN rail / Panel mount: 1G/2G	DIN rail / Panel mount: 1G/1G
TOD (End of Month)	Follows START Date and only runs when TOD >= START Date	Ignores START Date and always runs at the end of Month
Enable Outputs in STOP	Allowed when only local IO is configured	Not supported
Backup and restore	Yes	Yes
CPU clears Temp memory on each OB call		
• Optimized block (OB, FC, or FB)	Yes	Yes
• Non-optimized block (FC or FB)	Yes	No
SIMATIC Controller Profiling (https://support.industry.siemens.com/cs/ww/en/view/109750245)	No	Yes

Instruction set ¹ (Page 178)	S7-1200	S7-1200 G2
Legacy instructions		
• FieldRead, FieldWrite	Yes	Superseded by variable array index and multi-dimensional arrays
• CTRL_HSC	Yes	Superseded by CTRL_HSC_EXT
• "Point-to-Point" instructions	Yes	Superseded by "PtP Communication" instructions
• "USS" instructions	Yes	Superseded by "USS communication" instructions
• "MODBUS" instructions	Yes	Superseded by "MODBUS (RTU)" instructions
• TM_MAIL	Yes	Superseded by TMAIL_C

¹ Instruction groups indicate folders in the TIA Portal instruction task card

² These instructions are in the Extended instructions > Distributed I/O instructions

Instruction set ¹ (Page 178)	S7-1200	S7-1200 G2
Distributed I/O instructions		
• PROFIBUS ²	Yes	No
• AS-i control ²	Yes	No
Communication instructions		
• GPRSComm: CP1242-7	Yes	No
• OPC UA Server	Yes	Yes
• MODBUS TCP redundancy instructions	Yes	Yes
Safety instructions		
• RD_ARRAY_I	No	Yes
• RD_ARRAY_DI	No	Yes
• Range_16	No	Yes
Motion control instructions (Page 318)	Yes	Yes (different)
Alarming Instructions		
• Generate user message	Yes	Yes
• Generate program alarms	No	Yes
• Read status of program alarms	No	Yes
• Copy alarm to DB	No	Yes
• Acknowledge all alarms	No	Yes
• Read alarm resources	No	Yes
PID Instructions		
• Compact PID instructions	Yes	Yes
• Auxiliary functions instructions	Yes	Yes – adds instruction Filter_Universal
Instruction categories (folders in STEP 7 Instructions task card)		
• Process Image	No	Yes
• Module Parameterization	No	Yes
• Cryptography	No	Yes
• Time-based IO (requires IRT and special modules)	No	Yes

¹ Instruction groups indicate folders in the TIA Portal instruction task card

² These instructions are in the Extended instructions > Distributed I/O instructions

Instruction set ¹ (Page 178)	S7-1200	S7-1200 G2
• OPC UA	Yes	Yes
• Teleservice	Yes	No
Miscellaneous instructions in existing categories		
• Move: Array_DB and Symbolic Move instructions	No	Yes
• Convert: REF	No	Yes
• Program Control: INIT_RD and WAIT	No	Yes
• Date and time-of-day: T_COMP and TIME_TCK	No	Yes
• String + Char: S_COMP, JOIN, SPLIT, and GetSymbolForReference	No	Yes
• PROFIenergy: PE_START_END, PE_CMD, PE_DS3_Write_ET200S, and PE_WOL	No	Yes
• Interrupts: MSK_FLT, DMSK_FLT, READ_ERR, DIS_IRT, and EN_IRT	No	Yes
• Diagnostics: GetClock-Status, and GEN_DIAG	No	Yes
Data consistency for MOVE_BLK and MOVE_BLK_VARIANT	64 bytes	Element size

¹ Instruction groups indicate folders in the TIA Portal instruction task card

² These instructions are in the Extended instructions > Distributed I/O instructions

Quantities and default values	S7-1200	S7-1200 G2
Minimum cycle time	Disabled	Enabled (1 ms)
Communication Load	20%	20% See SIMATIC S7-1500, S7-1500R/H, ET 200SP, ET 200pro Cycle and response times (https://support.industry.siemens.com/cs/us/en/view/59193558/-158758826123)
Size of Internal Load Memory	4MB	8 MB

Quantities and default values	S7-1200	S7-1200 G2
HSC	6	8
PWM/PTO	4	8
Number of CPU connections	68	88
Number of active Trace jobs	2	4
Runtime meters	10	16
Hierarchical nesting depth of data type STRUCT	8	26 An array of STRUCT/UDT requires 3 hierarchical levels each. When using arrays of struct/UDT, the maximum nesting depth is reduced accordingly.

Legacy Scalance device support	S7-1200	S7-1200 G2
Scalance X005: 1P6GK50050BA001AA3	Yes	Not all
Scalance X310FE: 1P6GK53100BA002AA3	Yes	No

SIMATIC S7-1200 G2 data

The EU Data Act, a key component of the European data strategy, went into effect on January 11, 2024.

The following information provides an overview of the data that is generated by the SIMATIC S7-1200 G2 automation system and accessible to you.

E.1 CPU data

Type, format, and estimated scope of data that the product is capable of generating

Type of data	Formats	Estimated scope
Process data (input and output data, states, alarms)	Numeric formats, binary formats	Cyclic processing Depending on application
Configuration and program data (upload to programming device/PC)	Binary formats, string formats	Depending on application
Diagnostics data, system and security events, service data	Time formats, string formats, CSV, binary formats	Depending on application Several hundred bytes per event
Operating data (runtimes, cycle times, CPU utilization)	Numeric formats, time formats, JSON	Depending on application
Log data	Time formats, string formats, CSV	Depending on application

Continuous and real-time data generation

The SIMATIC S7-1200 G2 is able to generate data continuously and in real time. Data acquisition takes place continuously throughout the entire operation. The CPU operates with defined cycle times in which process data is acquired and processed.

Data storage and storage duration

Local data storage

The SIMATIC S7-1200 G2 stores data in integrated memory areas of the CPU and on the SIMATIC Memory Card.

Local data storage	Storage capacity	Storage duration
Load memory (with SIMATIC Memory Card)	Up to 32 Gbytes, depending upon SIMATIC Memory Card	Permanent
Program work memory	Up to 300 Kbytes, depending upon CPU	During operation of the CPU

Local data storage	Storage capacity	Storage duration
Data work memory	Up to 750 Kbytes, depending upon CPU	During operation of the CPU
Retentive memory	20 Kbytes	Permanent
NFC tag memory	8 Kbytes	While NFC is enabled in the STEP 7 program

More information

You can find more information on memory areas, retentivity, and memory usage in the SIMATIC S7-1200 G2 Programmable Logic Controller system manual (<https://support.industry.siemens.com/cs/us/en/view/109988293>), "CPU memory" section.

Remote data storage

Data can be transmitted to external systems through various communication interfaces of the SIMATIC S7-1200 G2, such as PROFINET, Industrial Ethernet.

The SIMATIC S7-1200 G2 can send data to various remote systems, including SCADA systems, SQL databases, cloud platforms (e.g. Insights Hub), and file servers.

The SIMATIC S7-1200 G2 can send logging data to a SIEM system in the form of syslog messages.

The storage duration on external systems depends on the configuration of the respective system.

The SIMATIC S7-1200 G2 CPU can be integrated as a data source into the Siemens Industrial Edge concept.

Data access/retrieval, terms of use, and quality of service

Type of data	Access/retrieval via	Terms of use	Quality of service*
Process data (input and output data, states, alarms)	TIA Portal Web server OPC UA HMI/SCADA systems CPU display	User management Authentication Certificates	Prioritization of control tasks over data access Data throughputs up to 1 Gbps via PROFINET Encrypted data transmission available (HTTPS, TLS)
Configuration and program data	TIA Portal Web server SIMATIC Memory Card	User management Authentication Certificates	Encrypted data transmission available (HTTPS, TLS)
Diagnostics data, system and security events, service data	TIA Portal SIMATIC Automation Tool Web server CPU display	User management Authentication Certificates	Encrypted data transmission available (HTTPS, TLS)
Operating data (runtimes, cycle times, CPU utilization)	TIA Portal Web server HMI/SCADA systems SIMATIC Controller Profiling	User management Authentication Certificates	Encrypted data transmission available (HTTPS, TLS)
Log data	TIA Portal Trace and logic analyzer function	User management Authentication	Encrypted data transmission available (HTTPS, TLS)

* "Quality of service" refers to the ability of the SIMATIC S7-1200 G2 to manage network resources efficiently and to ensure that specific performance requirements for data transmission are met.

Deletion of data from CPUs

To delete all data from the data memories of the CPU, the "Reset to factory settings" function is available.

A reset of the CPU to factory settings can be implemented using any of the following:

- Mode selector keys/switches of the CPU
- TIA Portal
- SIMATIC Automation Tool

More information

You can find more information on deleting data in the SIMATIC S7-1200 G2 Programmable Logic Controller system manual

(<https://support.industry.siemens.com/cs/us/en/view/109988293>), "Securely removing data" section or in the TIA Portal Information System.

E.2 Data of the interface and I/O modules

Type, format, and estimated scope of data that the product is capable of generating

Type of data	Formats	Estimated scope
Process data (input and output data, states, alarms)	Numeric formats, binary formats	Cyclic processing Depending on application
Configuration and parameter data (upload to programming device/PC)	Binary formats, string formats	Depending on application
Diagnostics data, service data	Binary formats	Depending on application Less than 100 bytes per diagnostic event; several kilobytes of service data
Fieldbus* metadata: I&M data, log data, statistics data	Binary formats, string formats	Approximately 100 bytes per read-out data record

* PROFIBUS, PROFINET, EtherNet/IP, Modbus TCP (only for interface modules as MultiFieldbus devices)

Continuous and real-time data generation

The interface and I/O modules are able to generate data continuously and in real time. Data acquisition takes place continuously throughout the entire operation. The cycle time is specified by the CPU.

Data access/retrieval, terms of use, and quality of service

Type of data	Access/retrieval by	Terms of use	Quality of service*
Process data (input and output data, states, alarms)	CPU TIA Portal SIMATIC Automation Tool PRONETA S7-PCT (for IO-Link masters) MFCT (for interface modules as MultiFieldbus devices)	Through fieldbus without authentication With CPU (Page 513)	Prioritization of control tasks over data access Standard fieldbus transmission mechanisms Data throughputs up to 1 Gbps through PROFINET
Configuration and parameter data (upload to programming device/PC)	TIA Portal (through CPU) S7-PCT (for IO-Link masters) MFCT (for interface modules as MultiFieldbus devices)	Through fieldbus without authentication With CPU (Page 513)	Standard fieldbus transmission mechanisms
Diagnostics data, service data	CPU TIA Portal SIMATIC Automation Tool PRONETA S7-PCT (for IO-Link masters) MFCT (for interface modules as MultiFieldbus devices)	Through fieldbus without authentication With CPU (Page 513)	Standard fieldbus transmission mechanisms
Fieldbus metadata: I&M data, log data, statistics data	CPU TIA Portal SIMATIC Automation Tool PRONETA S7-PCT (for IO-Link masters) MFCT (for interface modules as MultiFieldbus devices)	Through fieldbus without authentication With CPU (Page 513)	Standard fieldbus transmission mechanisms

* "Quality of service" refers to the ability of the interface, power supply, and I/O modules to manage network resources efficiently and to ensure that specific performance requirements for data transmission are met.

Deletion of data from interface and I/O modules**Interface modules**

To delete all data from the data memories of the interface module, the "Reset to factory settings" function is available.

A reset of the IM to factory settings can be implemented using any of the following:

- TIA Portal
- SIMATIC Automation Tool
- MultiFieldbus Configuration Tool (MFCT)
- PRONETA

I/O modules

The data of an IO-Link master can be deleted using S7-PCT by executing the "Reset to factory settings" function.

For all other I/O modules, no delete function is available.

More information

You can find more information on deleting data in the SIMATIC S7-1200 G2 Programmable Logic Controller system manual

(<https://support.industry.siemens.com/cs/ww/en/view/109988293>), "Securely removing data" topic and in the TIA Portal Information System.

Glossary

Alternate I/O active

Alternate I/O active means that every other input or output is active. Using alternate I/O reduces the concentration of heat around active circuits.

Autonegotiation

A signaling mechanism and procedure by which two connected devices choose common transmission parameters, such as speed, duplex mode, and flow control

In this process, the connected devices first share their capabilities regarding these parameters and then choose the highest performance transmission mode they both support.

AWG

American Wire Gauge: A standard, predominantly used in North America, that describes the size or diameter of single-stranded, solid, round electrical wire

CB

Communication board: A hardware component used to enable communication between the PLC and other devices or systems

CM

Communication module: A hardware component or device that facilitates communication between different systems, devices, or networks

CP

Communications Processor: A hardware component that facilitates Ethernet communications

CTS

Clear to Send: A control signal used in serial communication protocols to coordinate the flow of data between the transmitter and the receiver

When the transmitting device receives a CTS signal, it knows that the receiving device is clear to accept the data transmission.

DNS server

Domain Name System server: A directory of domain names that align with IP addresses

GSD file

General Station Description: Files provide detailed information about the device's capabilities, parameters, and communication properties, allowing the network configuration tool to properly integrate the device into the PROFINET network

IRT

Isochronous Real-Time: A transmission method by which PROFINET devices are synchronized with very high accuracy

MIB file

Management Information Base file: A database used for managing and monitoring network devices in a Simple Network Management Protocol (SNMP) system

NFC

Near Field Communication: A short-range wireless technology that enables devices to exchange data with each other by touching them together or bringing them into close proximity

OPC UA

Open Platform Communications Unified Architecture

Optimized DB

Data block with "Optimized block access" selected in the attributes of the Data block properties

An optimized data block maximizes performance, efficiency, and storage utilization.

PID

Proportional-Integral-Derivative: A control loop mechanism that employs feedback, widely used in industrial controls

RTC

Real-Time Clock or time of day clock: The CPU-supported clock that stores the calendar day, month, and year along with the time in hours, minutes, and seconds

RTS

Request to Send: A control signal used in serial communication protocols to coordinate the flow of data between the transmitter and the receiver

When the transmitting device sends an RTS signal, it indicates its intention to transmit data and requests permission from the receiving device.

TSAP

Transport Service Access Point: A unique address that identifies a specific communication endpoint within a PLC or other industrial devices

UART

Universal Asynchronous Receiver-Transmitter: A hardware component or interface used to facilitate serial communication between devices

Index

A

AC

- wiring and grounding prerequisites, 83
- isolation guidelines, 84
- grounding guidelines, 86
- wiring guidelines, 87

Active/passive communication

- connection IDs, 239
- parameters, 239

Add new device

- CPU, 161
- unspecific CPU, 163
- detect existing hardware, 163

Addressing

- memory areas and I/O in the PLC, 136

Ad hoc mode, TCP and ISO on TCP, 237

Air flow, 64

Altitude, 361

Analog I/O

- conversion to engineering units, 141
- configuration, 171
- status indicators, 333
- step response times (SB), 442
- voltage (inputs), 442-443
- current (inputs), 443
- current and voltage (outputs), 443-444
- step response times (SB), 474
- voltage (inputs), 475
- current (inputs), 475-476
- current and voltage (outputs), 476

Analog signal boards

- SB 1231 AI 4x14bit, 466
- SB 1232 AQ 4x14bit, 468
- SB 1233 AI 2x14bit / AQ 2x14bit, 470
- SB 1231 AI 4xTC, 478

Analog signal modules

- SM 1231 AI 8x14bit, 433
- SM 1232 AQ 8x14bit, 436
- SM 1233 AI 4x14bit / AQ 4x14bit, 438
- SM 1231 AI 8xTC, 445
- SM 1231 AI 4xRTD, 450

Approvals

- CE, 356
- cULus, 358
- ATEX, 359
- CCCEX approval, 360
- Australia and New Zealand - RCM Mark, 360
- Korea Certification, 360

Article numbers

- CPUs, 498
- Signal modules (SMs), 498
- Signal boards (SBs), 499
- Battery board (BB), 499
- Communication processor (CP), 499
- Communication module (CM), 499
- Communication board (CB), 499
- SIMATIC memory cards, 500
- input simulators, 500
- spare door kits, 500
- DIN rails, 500
- DIN rail end retainer, 500
- terminal block spare kits, 501
- STEP 7 programming software, 503

ATEX approval, 359

Atmospheric pressure, 361

Australia and New Zealand - RCM Mark approval, 360

Autonegotiation, 231

B

Backing up

- options, contents, and special considerations, 355

Battery board (BB)

- overview, 59
- BB 1297 Battery Board, 488
- inserting battery, 489

Biasing, 278

Blocks

- types of, 99
- function (FC), 101
- function block (FB), 101
- organization blocks (OBs), 106

Boards

- communication board (CB), [59](#)
- signal board (SB), [59](#)
- battery board (BB), [59](#)

Boolean or bit value access, [137](#)

Break, [288](#), [290](#)

Bus connector, [60](#)

C

Call structure local memory allocation, [139](#)

CE approval, [356](#)

Certificate parameters, [220](#)

Character position, message length, [293](#)

Character sequence

- message start , [290](#)
- message end, [294](#)

Clearance, airflow, and cooling, [64](#)

Client polling architecture, [302](#)

Clock

- memory bits, [132](#)
- CPU time-of-day clock, [135](#)

Cold junction compensation, thermocouple, [445](#), [477](#)

Communication

- Loss, pull or plug of modules, [113](#)
- communication load, [128](#)
- cycle time configuration, [128](#)
- PROFINET, [214](#)
- secure vs. legacy, [215](#)
- number of connections (PROFINET), [219](#)
- secure, [220](#)
- between CPUs and other devices, [220](#)
- network connection, [222](#)
- IP address, [227](#)
- MAC address, [227](#)
- connection IDs, [239](#)
- active/passive, configuring the partners, [239](#)
- TCON_Param, [239](#)
- Transport Layer Security (TLS), [240](#)
- network, [242](#)
- hardware connection, [243](#)
- active/passive, configuring the partners, [269](#)
- flow control, [285](#)
- send and receive parameters, [287](#)
- polling architecture, [302](#)
- CP 1243-1, [489](#)
- CM 1241 RS232/422/485, [491](#)
- CB 1241 RS485, [493](#)

Communication board (CB)

- overview, [59](#)
- device configuration, [158](#)
- adding modules, [165](#)
- configuration of parameters, [171](#)
- RS485, [277](#)
- LED indicators, [278](#)
- LED indicators, [331](#)
- CB 1241 RS485, [493](#)

Communication interfaces

- device configuration, [158](#)
- adding modules, [165](#)
- CM RS232/422/485, [277](#)
- CB RS485, [277](#)
- configuration, [282](#)
- 3964(R), [297](#)
- programming, [301](#)
- LED indicators, [331](#)

- Communication module (CM)
 - overview, [60](#)
 - power requirements, [68](#)
 - removal, [74](#)
 - installation, [74](#)
 - device configuration, [158](#)
 - adding modules, [165](#)
 - configuration of parameters, [171](#)
 - RS232/422/485, [277](#)
 - LED indicators, [278](#)
 - programming, [301](#)
 - LED indicators, [331](#)
 - CM 1241 RS232/422/485, [491](#)
 - Communication processor (CP)
 - device configuration, [158](#)
 - adding modules, [165](#)
 - configuration of parameters, [171](#)
 - CP 1243-1, [489](#)
 - Comparing and synchronizing code blocks for online/offline CPUs, [338](#)
 - Compatibility, [177](#)
 - Configuration
 - cycle time, [126](#)
 - communication load, [128](#)
 - startup parameters, [145](#)
 - discover, [163](#)
 - adding modules, [165](#)
 - CPU parameters, [166](#)
 - modules, [171](#)
 - network connection, [222](#)
 - PROFINET port, [227](#)
 - Ethernet port, [227](#)
 - IP address, [227](#)
 - MAC address, [227](#)
 - PLC to PLC communication, [248](#)
 - ports, [282](#)
 - communication interfaces, [282](#)
 - message receipt, [289](#)
 - 3964(R), communication interfaces/ports, [297](#)
 - 3964(R) priority and protocol parameters, [299](#)
 - Configuration"; "of transmitted message, [287](#)
 - Connections
 - types of communication, [214](#)
 - number of connections (PROFINET), [219](#)
 - connection IDs, [239](#)
 - configuration, [239](#)
 - partners, [269](#)
 - Connector, installation and removal, [79](#)
 - Contact information, [17](#)
 - Contamination level/overvoltage category, [364](#)
 - Cooling, [64](#)
 - Copying, cutting, and pasting in STEP 7, [177](#)
 - CP 1243-1, [276](#)
 - CP 1243-1 firmware update, [276](#)
 - CPU
 - version compatibility, [177](#)
 - CPU configuration
 - cycle time monitoring, [126](#)
 - operational parameters, [166](#)
 - communication to HMI, [246](#)
 - multiple CPUs, [248](#)
 - CPU memory card
 - inserting, [144](#)
 - transfer card, [146](#)
 - program card, [149](#)
 - CPUs
 - CPU 1212C AC/DC/RLY, [369](#)
 - CPU 1212C DC/DC/RLY, [369](#)
 - CPU 1212C DC/DC/DC, [369](#)
 - CPU 1212FC DC/DC/RLY, [380](#)
 - CPU 1212FC DC/DC/DC, [380](#)
 - CPU 1214C AC/DC/RLY, [391](#)
 - CPU 1214C DC/DC/RLY, [391](#)
 - CPU 1214C DC/DC/DC, [391](#)
 - CPU 1214FC DC/DC/RLY, [403](#)
 - CPU 1214FC DC/DC/DC, [403](#)
 - Creating a network connection
 - between PLCs, [222](#)
 - CTS (Hardware flow control, PtP), [285](#)
 - cULus approval, [358](#)
 - Current consumption, [68](#)
 - Cycle time
 - overview, [126](#)
 - configuration, [128](#)
 - Cyclic interrupt OB, [107](#)
- ## D
- Data block
 - overview, [99](#)
 - organization blocks (OBs), [106](#)
 - difference between global and instance, [136](#)
 - Data exchange between IO systems, [258](#)
 - Data transmission rate, [284](#), [298](#)

- DC
 - wiring and grounding prerequisites, [83](#)
 - isolation guidelines, [84](#)
 - grounding guidelines, [86](#)
 - wiring guidelines, [87](#)
 - inductive loads guidelines, [94](#)
 - outputs, [365](#)
- Debugging in RUN mode, [340](#), [348](#)
- Degree of protection, [364](#)
- Derating, [361](#)
 - CPU 1212C, [369](#)
 - CPU 1212FC, [381](#)
 - CPU 1214C, [392](#)
 - CPU 1214FC, [404](#)
- Device
 - PROFINET IO, [250](#)
 - PROFINET IO device names, [251](#)
- Device configuration, [158](#)
 - add new device, [161](#)
 - discover, [163](#)
 - adding modules, [165](#)
 - configuring the CPU, [166](#)
 - configuring the modules, [171](#)
 - network connection, [222](#)
 - PROFINET port, [227](#)
 - Ethernet port, [227](#)
- Diagnostic error interrupt OB, [111](#)
- Diagnostics
 - reducing security events, [133](#)
 - status LED indicators, [331](#)
- Diagnostics buffer
 - overview, [133](#)
- Digital I/O
 - configuration, [171](#)
 - pulse catch, [171](#)
- Digital signal boards
 - SB 1221 DI 8x24VDC, [456](#)
 - SB 1222 DQ 8x24VDC, [458](#)
 - SB 1223 DI 4x24VDC / DQ 4x24VDC, [460](#)
 - SB 1223 DI 4x5VDC / DQ 4x5VDC, [463](#)
- Digital signal modules
 - SM 1221 DI 16x24VDC, [414](#)
 - SM 1222 DQ 16x24VDC, [416](#)
 - SM 1222 DQ 16xRelay, [418](#)
 - SM 1223 DI 8x24VDC / DQ 8x24VDC, [420](#)
 - SM 1223 DI 8x24VDC / DQ 8xRelay, [423](#)
 - SM 1223 DI 16x24VDC / DQ 16x24VDC, [425](#)
 - SM 1223 DI 16x24VDC / DQ 16x24VDC Sink, [428](#)
 - SM 1223 DI 16x24VDC / DQ 16xRelay, [430](#)
- DIN rail, [63](#)
- Discover to upload an online CPU, [163](#)
- Displaying the MAC and IP addresses, [233](#), [245](#)
- Documentation, [17](#)
- Downloading
 - firmware update, [152](#)
 - displaying the MAC and IP addresses, [233](#)
 - displaying the MAC and IP addresses, [245](#)
- Download in RUN mode
 - overview, [340](#)
 - prerequisites, [341](#)
 - initiating from STEP 7, [341](#)
 - downloading selected blocks, [342](#)
 - compile errors, [344](#)
 - extended block interface, [345](#)
 - download without reinitialization, [345](#)
 - memory reserve and retentive memory reserve, [345](#)
 - global memory reserve settings, [347](#)
 - restrictions, [347](#)
 - failed download, [348](#)
 - considerations, [348](#)
- E**
- Edit in RUN mode, [340](#)
- Electromagnetic compatibility, [363](#)
- Electromagnetic compatibility (EMC), [363](#)
- End conditions, message, [292](#)
- Environmental conditions, [361](#)
- Errors
 - time errors, [110](#)
 - diagnostic errors, [111](#)
- Ethernet
 - types of communication, [214](#)
 - number of communication connections, [219](#)
 - switching, [221](#)
 - network connection, [222](#)
 - IP address, [227](#)
 - MAC address, [227](#)
 - overview, [235](#)
 - ad hoc mode, [237](#)
 - connection IDs, [239](#)
- Ethernet, instructions
 - GET (read data from a remote CPU) and PUT (write data to a remote CPU), [267](#)

Ethernet protocols, [235](#)
Event execution and queueing, [123](#)
Examples, communication
 PROFINET communication protocols, [235](#)
 I-device as IO device and IO controller, [257](#)
Examples, PtP communication
 start message condition, [291](#)
 message length within message, [293](#)
 end message condition, [295](#)
Examples, various
 analog value processing, [141](#)
 trace and logic analyzer function, [351](#)
Expanding the capabilities of the S7-1200 G2, [71](#)
Expansion modules, [71](#)
Extended block interface
 download in RUN mode, [345](#)
External power supply
 PM 1207, [497](#)

F

Fail-safe CPU
 Voltage, [70](#)
 memory cards, [157](#)
 CPU 1212FC, [380-381](#)
 CPU 1214FC, [403-404](#)
Fail-safe device
 Voltage, [70](#)
FB (function block), [99](#)
FC (function), [99](#)
Firmware update
 with a memory card, [152](#)
First scan indicator, [132](#)
Fixed length, [293](#)
Flow control
 configuration, [285](#)
 managing, [285](#)
Flow control, [285](#)
Forcing values, [339](#)
Freeport protocol, [281](#)
Frequency, clock bits, [132](#)
Function (FC)
 overview, [99](#)
Functionality, I-device, [253](#)

Function block (FB)
 overview, [99](#)

G

GET (read data from a remote CPU), [267](#)
Global data block, [136](#)
Global library
 USS protocol overview, [303](#)
GSD file, [262](#)
Guidelines
 installation procedures, [63](#)
 installation, [64](#)
 CPU installation, [71](#)
 wiring and grounding prerequisites, [83](#)
 isolation, [84](#)
 grounding, [86](#)
 wiring, [87](#)
 inductive loads, [94](#)
 lamp loads, [96](#)

H

Hardware configuration, [158](#)
 add new device, [161](#)
 discover, [163](#)
 adding modules, [165](#)
 configuring the CPU, [166](#)
 configuring the modules, [171](#)
 network connection, [222](#)
 PROFINET port, [227](#)
 Ethernet port, [227](#)
Hardware flow control, [285](#)
Hardware interrupt OB, [108](#)
HMI devices
 network connection, [222](#)
 configuring PROFINET communication, [246](#)

- I
- I/O
 - inductive loads guidelines, [94](#)
 - addressing, [140](#)
 - analog status indicators, [333](#)
 - monitoring with a watch table, [339](#)
 - forcing values, [339](#)
 - step response times (SB), [442](#)
 - analog input voltage, [442-443](#)
 - analog input current, [443](#)
 - analog output current and voltage, [443-444](#)
 - step response times (SB), [474](#)
 - analog input voltage, [475](#)
 - analog input current, [475-476](#)
 - analog output current and voltage, [476](#)
- I/O access error OBs, [122](#)
- I-device (intelligent IO device)
 - functionality, [253](#)
 - lower-level PN IO system, [255](#)
 - configuring, [260](#)
 - configuring with GSD file, [262](#)
- Idle line, [288](#), [290](#)
- Incompatible CPU version error, [336](#)
- Inductive loads guidelines, [94](#)
- Industrial environments, approvals, [361](#)
- Information resources, [17](#)
- Inputs and outputs
 - pulse catch bits, [169](#)
- Input simulators
 - eight position, [495](#)
 - fourteen position, [495](#)
- Inserting a device
 - unspecific CPU, [163](#)
- Inserting the memory card into CPU, [144](#)
- Installation
 - signal modules (SM), [60](#)
 - overview, [63](#)
 - overview, [64](#)
 - guidelines, [64](#)
 - cooling, [64](#)
 - air flow, [64](#)
 - clearance, [64](#)
 - thermal zone, [64](#)
 - thermal zone, [67](#)
 - mounting dimensions, [67](#)
 - CPU, [71](#)
 - communication module (CM), [74](#)
 - signal board (SB), [77](#)
 - terminal block connector, [79](#)
 - wiring and grounding prerequisites, [83](#)
 - isolation guidelines, [84](#)
 - grounding guidelines, [86](#)
 - wiring guidelines, [87](#)
 - inductive loads guidelines, [94](#)
 - lamp loads guidelines, [96](#)
- Instance data block, [136](#)
- Instructions
 - common parameters, [241](#)
 - PtP, [300](#)
 - USS, [305](#)
 - MODBUS TCP, [310](#)
 - Modbus RTU, [313](#)
- Insulation, [364](#)
- Inter-character timeout, [293](#)
- Interrupts
 - overview, [106](#)
 - interrupt latency, [123](#)
- IO system, data exchange, [258](#)
- IP address, [166](#)
 - device configuration, [166](#)
 - Assigning, [224](#)
 - assigning to an online CPU, [226](#)
 - configuring, [227](#)
 - MAC address, [227](#)
 - displaying and downloading, [233](#)
 - assigning, [245](#)
 - displaying and downloading, [245](#)
- IP address, emergency (temporary), [272](#)
- IP router, [227](#)
- Isochronous Real-Time PROFINET (IRT), [265](#)

Isolation guidelines, [84](#)

ISO on TCP
ad hoc mode, [237](#)

ISO-on-TCP
connection IDs, [239](#)
parameters, [239](#)

ISO on TCP protocol, [235](#)

K

Know-how protection, [210](#)

Know-how protection for blocks
Setting up, [211](#)
Changing, [212](#)
Removing, [213](#)

Korea Certification approval, [360](#)

L

LAD (ladder logic)
status, [339](#)

Lamp loads guidelines, [96](#)

Latency, [123](#)

LED indicators
communication interfaces, [278](#)
CPU status, [331](#)
communication interface, [331](#)

Legacy communication, [215](#)

Length, PtP message, [293](#)

License conditions and copyrights (LCC), [156](#)

Load memory, [129](#)

Local/Partner connection, [223](#)

Local memory
maximum per OB priority level, [139](#)
usage by blocks, [139](#)

Logic analyzer, [350](#)

LookAhead OB, [120](#)

Loss of CPU communication to modules, [113](#)

Lost password, [156](#)

M

MAC address
locating, [223](#)
configuration, [227](#)
displaying and downloading, [233](#)

Manuals, [17](#)

MC_LookAhead OB, [120](#)

MC-PostServo OB, [119](#)

MC-PreServo OB, [119](#)

Measurements, trace jobs, [351](#)

Media Redundancy with Planned Duplication (MRPD), [264](#)

Memory

load, work, and retentive, [129](#)
system and clock memory, [131](#)
L (local memory), [136](#)
I (process image input), [138](#)
Q (process image output), [138](#)
M (bit memory), [139](#)
temp memory, [139](#)

Memory areas

process image and physical access, [136](#)
addressing Boolean or bit values, [137](#)

Memory card

overview, [143](#)
inserting into CPU, [144](#)
configure the startup parameters, [145](#)
transfer card, [146](#)
program card, [149](#)
firmware update, [152](#)
Protection of confidential PLC configuration data, [154](#)
empty transfer card for a lost password, [156](#)
transferring license conditions and copyrights, [156](#)
fail-safe CPUs, [157](#)
incompatibility error, [336](#)

Memory card service life, [151](#)

Memory location access, [136](#)

Message conditions

start, [290](#)
end, [292](#)

Message configuration

transmit (send) parameters, [287](#)
receipt parameters, [289](#)
instructions, [301](#)

Message receipt configuration

PtP device configuration, [289](#)

Modbus

function codes, [308](#)
memory addresses, [309](#)

Modbus RTU

- overview, [312](#)
- instructions, [313](#)
- instruction library versions, [314](#)
- maximum Modbus slaves, [314](#)

Modbus TCP

- overview, [309](#)
- maximum number of connections, [309](#)

MODBUS TCP

- instructions, [310](#)

Modbus TCP Redundancy instructions, [311](#)**Modifying**

- watch table, [339](#)

Modules

- communication module (CM), [60](#)
- signal modules (SM), [60](#)
- thermal zone, [64](#)
- thermal zone, [67](#)
- configuring parameters, [171](#)

Monitoring

- watch table, [339](#)
- force table, [339](#)

Mounting

- overview, [63](#)
- guidelines, [64](#)
- airflow, clearance, cooling, and thermal zone, [64](#)
- airflow, clearance, cooling, and thermal zone, [67](#)
- dimensions, [67](#)
- CPU, [71](#)
- module, communication (CM) and signal (SM), [74](#)
- board, signal (SB), [77](#)
- terminal block connector, [79](#)
- wiring and grounding prerequisites, [83](#)
- isolation guidelines, [84](#)
- grounding guidelines, [86](#)
- wiring guidelines, [87](#)
- inductive loads guidelines, [94](#)
- lamp loads guidelines, [96](#)

MRP (Media Redundancy Protocol), [264](#)**N****Near Field Communication (NFC)**

- overview, [315](#)

Network communication, [242](#)**Network connection**

- connecting devices, [222](#)
- multiple CPUs, [250](#)

Network time protocol (NTP), [235](#)**O****OBs, [106](#)****Online**

- assigning an IP address to a CPU, [226](#)
- comparing and synchronizing code blocks, [338](#)
- tools, [338](#)
- watch table, [339](#)
- forcing values, [339](#)
- downloading in RUN mode, [340](#)

OPC UA server, [273](#)

- features, [273](#)
- configuration, [273](#)
- limitations (interface, method, and subscription), [274](#)
- security, [275](#)

Opening know-how protected blocks, [212](#)**Open-source software (OSS), [156](#)****Open User Communication instructions return values, [241](#)****Operating conditions, [361](#)****Operating environment**

- CPU 1212C, [369](#)
- CPU 1212FC, [381](#)
- CPU 1214C, [392](#)
- CPU 1214FC, [404](#)

Operating mode

- operating modes of the CPU, [101](#)

Organization block

- overview, [99](#)
- startup processing, [104](#)
- processing, [106](#)
- priority classes, [106](#)
- calling and functionality, [106](#)
- cyclic interrupt, [107](#)
- temp memory allocation, [139](#)

Overvoltage category, [364](#)**P****Parity, [285](#)**

- Passive/active communication
 - connection IDs, [239](#)
 - parameters, [239](#)
- Password protection
 - empty transfer card, [156](#)
 - lost password, [156](#)
- Password provider, [210](#)
- Phase shift, cyclic interrupt OBs, [107](#)
- PID
 - PID_Compact algorithm, [328](#)
 - PID_3Step algorithm, [328](#)
- PLC
 - overview of features, [57](#)
 - cycle time, [126](#)
 - cycle time configuration, [128](#)
 - communication load, [128](#)
 - tag table, [136](#)
 - adding modules, [165](#)
 - assigning an IP address to an online CPU, [226](#)
- PM 1207 power module, [497](#)
- Point-to-Point communication
 - Freeport, [281](#)
 - programming, [301](#)
- Polling architecture, [302](#)
- Pollution degree, [364](#)
- Portal view, [97](#)
- Port configuration, [282](#)
 - 3964(R), [297](#)
 - instructions, [301](#)
- Port numbers
 - assigning to communication partners, [235](#)
 - restricted, [242](#)
- Power budget
 - overview, [68](#)
- Power module (PM)
 - PM 1207, [497](#)
- Priority class for OBs
 - overview, [106](#)
 - event execution and queuing, [124](#)
- Process image
 - forcing values, [339](#)
- Profile OB, [117](#)
- PROFINET
 - configuring the IP address, [166](#)
 - time synchronization, [166](#)
 - types of communication, [214](#)
 - number of communication connections, [219](#)
 - network connection, [222](#)
 - IP address, [227](#)
 - MAC address, [227](#)
 - Ethernet address properties, [228](#)
 - system startup time, [234](#)
 - device naming and addressing, [234](#)
 - IP address assignment, [234](#)
 - overview, [235](#)
 - ad hoc mode, [237](#)
 - connection IDs, [239](#)
 - testing a network, [245](#)
 - configuring communication between CPU and HMI device, [246](#)
 - PLC-to-PLC communication, [248](#)
 - CPU-to-CPU communication, [248](#)
 - network connection, [250](#)
- PROFINET, instructions
 - GET (read data from a remote CPU) and PUT (write data to a remote CPU), [267](#)
- PROFINET IO
 - adding a device, [250](#)
 - assigning a CPU and device name, [251](#)
- PROFINET port
 - autonegotiation, [231](#)
- PROFINET RT, [235](#)
- Program
 - organization blocks (OBs), [106](#)
 - priority class, [106](#)
- Program card
 - overview, [143](#)
 - configure the startup parameters, [145](#)
 - creating, [149](#)
- Program cycle OB, [106](#)
- Program execution, [101](#)
- Programming
 - operating modes of the CPU, [101](#)
 - priority class, [106](#)
 - unspecific CPU, [163](#)
 - PtP instructions, [301](#)
 - PID_Compact algorithm, [328](#)
 - PID_3Step algorithm, [328](#)
 - comparing and synchronizing code blocks, [338](#)

Project
 transfer card, [146](#)
 program card, [149](#)
 comparing and synchronizing code blocks, [338](#)

Project view, [97](#), [98](#)

Protection, [206](#)
 Access levels, [207](#)
 Behavior of a password-protected CPU, [209](#)
 Know-how protection, [211](#)

Protection class, [364](#)

Protection concept, [190](#)

Protection level
 lost password, [156](#)

Protection of confidential PLC configuration data
 SIMATIC memory card, [154](#)

Protocol
 PROFINET RT, [235](#)
 TCP and ISO on TCP, [235](#)
 UDP, [235](#)
 communication, [281](#)
 Freeport, [281](#)
 Modbus, [281](#)
 USS, [281](#)

PtP
 configuring ports, [282](#)
 configuring parameters, [287](#)
 3964(R), configuring ports, [297](#)
 3964(R), configuring priority and protocol parameters, [299](#)
 instructions, [300](#)
 programming, [301](#)

PtP"; "communication, [281](#)

Pull or plug of modules OB, [113](#)

Pulse
 catch bits, digital input configuration, [169](#)

Pulse catch, [171](#)

PUT (write data to a remote CPU), [267](#)

Q

Queueing, [123](#)

R

Rack or station failure OB, [114](#)

Rated voltages, [365](#)

Real-time clock
 BB 1297 Battery Board, [489](#)

Redundancy
 MRP, [264](#)
 MRPD, [264](#)

Relay electrical service life, [366](#)

Restricted TSAPs and port numbers, [242](#)

Retentive block tags
 download in RUN mode, [346](#)

Retentive memory, [129](#)

Return values
 Open User Communication instructions, [241](#)

Reverse voltage protection, [365](#)

Router IP address, [228](#)

RS232/422/485 communication module, [277](#)

RTS (Hardware flow control, PtP), [285](#)

RTS On delay, Off delay, [288](#)

RUN mode, [101](#), [105](#)

S

S7 routing, [265](#)

Safety information, [65](#)

SB 1231 AI 4xRTD, [483](#)

Scan cycle
 overview, [126](#)

Secure communication, [215](#), [220](#)

Security
 reducing events in diagnostic buffer, [133](#)
 lost password, [156](#)
 secure vs. legacy communication, [215](#)

Send message configuration, [287](#)

Serial communication, [281](#)

Service and support, [17](#)

Shared device
 concept, [263](#)

Shielded connections, grounding guidelines, [86](#)

- Signal boards (SB)
 - overview, [59](#)
 - power requirements, [68](#)
 - installation, [77](#)
 - removal, [77](#)
 - adding modules, [165](#)
 - configuration of parameters, [171](#)
 - SB 1221 DI 8x24VDC, [456](#)
 - SB 1222 DQ 8x24VDC, [458](#)
 - SB 1223 DI 4x24VDC / DQ 4x24VDC, [460](#)
 - SB 1223 DI 4x5VDC / DQ 4x5VDC, [463](#)
 - SB 1231 AI 4x14bit, [466](#)
 - SB 1232 AQ 4x14bit, [468](#)
 - SB 1233 AI 2x14bit / AQ 2x14bit, [470](#)
 - SB 1231 AI 4xTC, [478](#)
- Signal boards (SBs) and signal modules (SMs)
 - analog input voltage, [442-443](#)
 - analog input current, [443](#)
 - analog output current and voltage, [443-444](#)
 - analog input voltage, [475](#)
 - analog input current, [475-476](#)
 - analog output current and voltage, [476](#)
- Signal modules (SM)
 - SM 1221 DI 16x24VDC, [414](#)
 - SM 1222 DQ 16x24VDC, [416](#)
 - SM 1222 DQ 16xRelay, [418](#)
 - SM 1223 DI 8x24VDC / DQ 8x24VDC, [420](#)
 - SM 1223 DI 8x24VDC / DQ 8xRelay, [423](#)
 - SM 1223 DI 16x24VDC / DQ 16x24VDC, [425](#)
 - SM 1223 DI 16x24VDC / DQ 16x24VDC Sink, [428](#)
 - SM 1223 DI 16x24VDC / DQ 16xRelay, [430](#)
 - SM 1231 AI 8x14bit, [433](#)
 - SM 1232 AQ 8x14bit, [436](#)
 - SM 1233 AI 4x14bit / AQ 4x14bit, [438](#)
 - SM 1231 AI 8xTC, [445](#)
 - SM 1231 AI 4xRTD, [450](#)
- Signal modules (SM), general
 - CPU expansion, [60](#)
 - power requirements, [68](#)
 - adding modules, [165](#)
 - configuration of parameters, [171](#)
- Simulators, [495](#)
- Slave polling architecture, [302](#)
- SM 1231 RTD
 - selection tables, [452](#)
- SM and SB
 - device configuration, [158](#)
- SNMP, enabling and disabling, [266](#)
- Snubber circuits for inductive loads, [94](#)
- Software flow control, [286](#)
- Specifications
 - general technical specifications, [356](#)
 - approvals, [356](#)
 - industrial environments, [361](#)
 - environmental conditions, [361](#)
 - electromagnetic compatibility (EMC), [363](#)
 - rated voltages, [365](#)
 - CPU 1212C AC/DC/RLY, [369](#)
 - CPU 1212C DC/DC/RLY, [369](#)
 - CPU 1212C DC/DC/DC, [369](#)
 - CPU 1212FC DC/DC/RLY, [380](#)
 - CPU 1212FC DC/DC/DC, [380](#)
 - CPU 1214C AC/DC/RLY, [391](#)
 - CPU 1214C DC/DC/RLY, [391](#)
 - CPU 1214C DC/DC/DC, [391](#)
 - CPU 1214FC DC/DC/RLY, [403](#)
 - CPU 1214FC DC/DC/DC, [403](#)
 - step response times (SB), [442](#)
 - analog input voltage, [442-443](#)
 - analog input current, [443](#)
 - analog output current and voltage, [443-444](#)
 - step response times (SB), [474](#)
 - analog input voltage, [475](#)
 - analog input current, [475-476](#)
 - analog output current and voltage, [476](#)
 - SB 1231 AI 4xTC, [478](#)
 - input simulators, [495](#)
- Start conditions, message, [290](#)
- Start message character, [290](#)
- Startup
 - startup processing, [104](#)
- Startup after POWER ON, [101](#)
- Startup OB, [107](#)
- Startup parameters, [145](#)
- Status LEDs
 - communication interfaces, [278](#)
 - CPU, [331](#)
- Status OB, [116](#)

STEP 7

- view (Portal and Project), [97](#)
- code blocks, [99](#)
- operating modes of the CPU, [101](#)
- priority class, [106](#)
- cycle time, [126](#)
- cycle time configuration, [128](#)
- communication load, [128](#)
- configuring devices, [158](#)
- adding devices, [161](#)
- adding devices, [165](#)
- configuring devices, [166](#)
- configuring devices, [171](#)
- version compatibility, [177](#)
- network connection, [222](#)
- assigning an IP address to an online CPU, [226](#)
- PROFINET port, [227](#)
- Ethernet port, [227](#)
- adding devices, [250](#)
- comparing and synchronizing code blocks, [338](#)
- forcing values, [339](#)

Stop bits, [285](#)

STOP mode, [101](#)

Subnet mask, [227](#)

Support, [17](#)

Suppressor circuits for inductive loads, [94](#)

Syslog

- configuration, [168](#)

- ports, [217](#)

System memory byte, [132](#)

T

TCON

- connection IDs, [239](#)

- connection parameters, [239](#)

TCON_Param, [239](#)

TCP

- protocol, [235](#)

- ad hoc mode, [237](#)

- connection IDs, [239](#)

- parameters, [239](#)

TCP/IP communication, [235](#)

Technical specifications, [356](#)

TeleControl

- communication processor, [276](#)

Temp memory

- maximum per OB priority level, [139](#)

- usage by blocks, [139](#)

Terminal block connectors

- removing and installing, [79](#)

- wiring and unwiring, [88](#)

- article numbers for spare kits, [501](#)

Terminating a network connector, [278](#)

Thermal zone, [64](#), [67](#)

Thermocouple

- basic operation, [445](#)

- cold junction compensation, [445](#)

- basic operation, [477](#)

- cold junction compensation, [477](#)

- SB 1231 AI 4xTC, [478](#)

- SB 1231 selection table, [479-480](#)

- SB 1231 Filter selection table, [480](#)

TIA Portal, Portal view and Project view, [97](#)

Time delay Interrupt OB, [107](#)

Time error interrupt OB, [110](#)

Time of day OB, [115](#)

Time synchronization

- setting the time-of-day clock, [175](#)

Topology

- view, [98](#)

Trace feature, [350](#)

Transfer card, [143](#)

- overview, [143](#)

- configure the startup parameters, [145](#)

- empty transfer card for a lost password, [156](#)

Transmission block (T-block), [249](#)

Transmit message configuration

- PtP device configuration, [287](#)

TRCV_C (receive data via Ethernet, TCP)

- ad hoc mode, [237](#)

- connection IDs, [239](#)

- connection parameters, [239](#)

TRCV (receive data via Ethernet, TCP)

- ad hoc mode, [237](#)

- connection IDs, [239](#)

Triggering

- trace, [350](#)

Troubleshooting

- LED indicators, [331](#)

TSAP (transport service access points)
 configuring general parameters, [249](#)
 TSAP (transport service access points)
 instructions for assigning to devices, [235](#)
 definition, [237](#)
 restricted TSAPs and port numbers, [242](#)
 TSEND_C (send data via Ethernet, TCP)
 connection IDs, [239](#)
 connection parameters, [239](#)
 TSEND (send data via Ethernet, TCP)
 connection IDs, [239](#)
 TURCV (receive data via Ethernet, UDP)
 connection parameters, [239](#)
 TUSEND (send data via Ethernet, UDP)
 parameters, [239](#)

U

UDP
 protocol, [235](#)
 parameters, [239](#)
 Unknown CPU version error, [336](#)
 Unspecific CPU, [163](#)
 Update OB, [117](#)
 Updating firmware
 with a memory card, [152](#)
 User interface of STEP 7, [97](#)
 User program
 organization blocks (OBs), [106](#)
 USS
 instructions, [305](#)
 USS protocol library
 overview, [303](#)
 instruction versions, [304](#)
 requirements for using, [304](#)
 status codes, [306](#)

W

Wait time, [285](#)
 Warm restart, [101](#)
 Watch table
 using, [339](#)
 Wiring diagrams
 SM 1221 DI 16x24VDC, [415](#)
 SM 1222 DQ 16x24VDC, [418](#)
 SM 1222 DQ 16xRelay, [420](#)
 SM 1223 DI 8x24VDC / DQ 8x24VDC, [422](#)
 SM 1223 DI 8x24VDC / DQ 8xRelay, [424](#)
 SM 1223 DI 16x24VDC / DQ 16x24VDC, [427](#)
 SM 1223 DI 16x24VDC / DQ 16x24VDC Sink, [429](#)
 SM 1223 DI 16x24VDC / DQ 16xRelay, [432](#)
 SM 1231 AI 8x14bit, [435](#)
 SM 1232 AQ 8x14bit, [437](#)
 SM 1233 AI 4x14bit / AQ 4x14bit, [440](#)
 SM 1231 AI 8xTC, [449](#)
 SM 1231 AI 4xRTD, [454](#)
 SB 1221 DI 8x24VDC, [457](#)
 SB 1222 DQ 8x24VDC, [460](#)
 SB 1223 DI 4x24VDC / DQ 4x24VDC, [462](#)
 SB 1223 DI 4x5VDC / DQ 4x5VDC, [465](#)
 SB 1231 AI 4x14bit, [468](#)
 SB 1232 AQ 4x14bit, [470](#)
 SB 1233 AI 2x14bit / AQ 2x14bit, [474](#)
 SB 1231 AI 4xTC, [482](#)
 SB 1231 AI 4xRTD, [487](#)
 CP 1243-1, [490](#)
 CM 1241 RS232/422/485, [492-493](#)
 CB 1241 RS485, [494-495](#)
 Wiring guidelines, [64](#)
 clearance for airflow and cooling, [64](#)
 prerequisites, [83](#)
 grounding, [86](#)
 Work memory, [129](#)

X

XON / XOFF, [286](#)